# SEPPmail

Version 7.2

## Benutzerhandbuch
## mit Ruleset

**SEPPmail AG**
Industriestrasse 7
CH-5432 Neuenhof

+41 56 648 28 38 fon
+41 56 648 28 39 fax
info@seppmail.ch mail

www.seppmail.ch

# Inhaltsverzeichnis


**Part I Vorwort 8**

**Part II Einleitung 10**

**1 Dokumentationsvereinbarungen ... 11**
**2 Sichere E-Mail-Kommunikation durch Verschlüsselung ... 12**
**3 Digitale E-Mail-Signaturen ... 15**
**4 Zentrale Firmen E-Mail Fussnote ... 16**
**5 Kompatibilität zu anderen Secure E-Mail Systemen ... 16**
**6 Remote-Administration mittels Web-Portal ... 16**

**Part III Die SEPPmail-Appliance 17**

**1 SEPPmail AG (Hersteller) ... 17**
**2 Vorstellung und Verfahren ... 18**
Produktphilosophie ... **18**
Fünf generische Prinzipien ... 18
Verschlüsselungstechnologien ... **20**
S/MIME (X.509) ... 20
Managed PKI ... 20
OpenPGP ... 20
LDAP Key-Lookup für S/MIME und OpenPGP ... 21
TLS ... 21
Gateway-to-Gateway (Domänen-) Verschlüsselung ... **21**
Verschlüsselungshierarchie ... **22**
GINA Webmail ... **23**
Mobile Computing Support ... 33
Interne Nutzer von mobilen Endgeräten ... 33
Externe Empfänger von verschlüsselten E-Mails auf mobilen Endgeräten ... 34
Kompatibiolitätsmatrix für Empfänger von GINA Web-Mails ... 34
Administration und Management ... 35
MS-Outlook AddIn ... 35
Elektronische Signaturen ... **35**
**3 Aufbau und Architektur ... 36**
Appliance ... **36**
Hardwaremodelle ... 36
Virtualisierte Versionen ... 37
Software ... **38**
Zentrales Regelwerk (Rule Engine) ... **38**
Architekturen ... **39**
Im vollen Mailstrom ... 39
Kleine Umgebungen ... 39
Grössere beziehungsweise komplexere Umgebungen ... 40
Über spezielles Routing angesteuert ... 41
Schnittstellen ... 41
Hochverfügbarkeit, Loadbalancing ... **42**


© 2015 SEPPmail AG

Multi Master LDAP ... 42
Queue-Less-Betrieb ... 42
Cluster: Multimaster LDAP & Queue-Less Betrieb ... 42
Fail-Over und Loadbalancing ... 42
System Management ... 44
Administration ... 44
Rollenrechte ... 44
Backup / Restore ... 45
Systemupdate ... 45
SysLog ... 45
Report ... 45
Mandantenfähigkeit - Public-/Private Cloud Implementierung ... 47
4 Sicherheit ... 48
5 Zusätzliche Features ... 50
Large File Management (LFM) ... 50
Internal Mail Encryption (IME) ... 53
Self Service Password Management (SSPM) ... 56
Protection Pack (VSPP) ... 56
6 Lizenzen ... 57
Basissysteme und Lizenz ... 57
Protection Pack (VSPP) ... 57
Signatur und Verschlüsselung ... 57
Large File Management (LFM) ... 58
Self Service Password Management (SSPM) ... 58
Internal Mail Encryption (IME) ... 58
Part IV Inbetriebnahme der Secure E-Mail-Gateway-Appliance 59
1 Bevor Sie beginnen ... 59
2 Integration der SEPPmail-Appliance in Ihre E-Mail-Umgebung (Standard Konfiguration) ... 60
3 Benötigte Informationen zur Inbetriebnahme ... 61
4 Firewall / Router einrichten ... 63
5 SEPPmail-Appliance anschliessen ... 65
6 Basiskonfiguration in wenigen Schritten ... 66
Netzwerkeinstellungen und Systemregistrierung ... 66
Initialer Verbindugsaufbau ... 66
Hardware Appliance ... 66
Virtuelle Appliance ... 67
Consolen Login ... 68
Login als Administrator ... 70
Netzwerkeinstellungen der SEPPmail-Appliance ... 70
Netzwerkkonfiguration prüfen ... 71
Das System registrieren ... 72
Das System auf den neusten Stand bringen ... 72
Wichtige Sicherheitsmassnahmen ... 73
Administrator-Kennwort ändern ... 73
Festlegen des HTTPS-Protokolls für den sicheren Zugriff zum System ... 73
Backup Benutzer erstellen ... 73
Eingabe der Postmaster Adresse für den Empfang von Systemmeldungen ... 74
7 Vorbereiten der GINA-Technologie ... 75

© 2015 SEPPmail AG

**8 Integration in die bestehende E-Mail Infrastruktur ... 76**
Zu verwaltende E-Mail-Domänen einrichten ... 76
Ausgehenden E-Mail-Verkehr steuern ... 76
Mail Relaying ... 76
SSL-Zertifikat einbinden ... 77
SSL-Device-Zertifikat selbst erstellen ... 77
SSL-Device-Zertifikat von einer öffentlichen Zertifizierungsstelle anfordern ... 78
Bestehendes SSL-Device-Zertifikat verwenden ... 80
E-Mail-Datenfluss umstellen ... 82
IronPort Anbindung der SEPPmail ... 83
Steuern der Appliance ... 86
**9 Clustern mehrer Systeme ... 87**
Allgemein ... 87
Hochverfügbarkeits Cluster ... 89
Loadbalancing Cluster ... 91
Aufteilen des Ein- und Ausgehenden Verkehrs ... 91
Nutzen des DNS Round Robin Verfahrens ... 93
Nutzen eines externen Loadbalancers ... 95
Geo Cluster ... 97
Frontend/Backend Cluster ... 98
Secure Webmail Satellite ... 99
Unterstützen externer redundanter Systeme ... 100
**10 Einrichten zusätzlicher Features ... 101**
Protection Pack (VSPP) ... 101
Internal Mail Encryption (IME) ... 101
Self Service Password Management (SSPM) ... 102
Large File Management (LFM) ... 102

**Part V Administrative Aufgaben 103**

**Part VI Microsoft Outlook AddIn 104**

**1 Einleitung ... 104**
**2 Download ... 104**
**3 Systemanforderungen ... 105**
**4 Installation ... 105**
Interaktive Installation ... 106
Silent Installation ... 108
Deinstallation ... 109
**5 Registry ... 110**
**6 AddIn Verwaltung ... 112**

**Part VII Referenz der Menüpunkte 113**

**1 Übersicht der Menüpunkte ... 113**
**2 Login/Logout ... 115**
**3 Home ... 116**
**4 System ... 119**
**5 Mail System ... 129**
Untermenü Add/Edit Managed Domain ... 136
Untermenü Import openPGP Key ... 141

© 2015 SEPPmail AG

Untermenü Import S/MIME Key ... 142
Untermenü Add TLS Domain ... 143
6 MailProcessing ... 147
Untermenü Create new GINA Domain ... 164
Untermenü Edit GINA Settings ... 165
Untermenü Edit GINA Layout ... 172
Untermenü Edit Translations ... 176
Untermenü Edit Disclaimer ... 178
7 SSL ... 179
Untermenü Request a new Certificate ... 181
Untermenü Download and Import signed Certificate ... 183
8 CA ... 185
9 Administration ... 190
Untermenü Register this device ... 193
10 Cluster ... 195
11 Logs ... 199
12 Statistics ... 201
13 Users ... 203
Untermenü Benutzerdetails ... 204
Untermenü Create new user account ... 208
Untermenü Password Policy ... 209
14 GINA Accounts ... 210
Untermenü Benutzer-Details ... 211
15 Groups ... 213
16 LFM accounts ... 215
17 OpenPGP public keys ... 216
18 X.509 Certificates ... 217
19 X.509 Root Certificates ... 218
Untermenü Vertrauensstellung ... 219
20 Domain Certificates ... 221
21 Customers ... 223
Untermenü Create new / Edit Settings for customer ... 224
Manage GINA accounts ... 226

Part VIII Referenz der Regelwerk-Anweisungen 228

1 Allgemeine Informationen ... 228
2 Kontrollstrukturen - if/else Anweisungen ... 230
3 Allgemeine Befehle ... 231
add_rcpt() ... 231
authenticated() ... 232
compare() ... 234
compareattr() ... 236
comparebody() ... 237
disclaimer() ... 238
from_managed_domain() ... 239
incoming() ... 240
log() ... 241
logheader() ... 242

© 2015 SEPPmail AG

logsubject() ... 243
normalize_header() ... 244
notify() ... 245
replace_rcpt() ... 247
replace_sender() ... 248
rmatch() ... 249
rmatchsplit() ... 250
rmheader() ... 251
setheader() ... 252
tagsubject() ... 253
tag_subject() ... 253
**4 Befehle für die Benutzerverwaltung ... 254**
createaccount() ... 254
member_of() ... 255
setuserattr() ... 256
**5 Befehle für die Zertifikatsverwaltung ... 257**
attachpgpkey() ... 257
has_smime_key() ... 257
smime_create_key() ... 258
**6 Befehle für das Handhaben von Nachrichten ... 259**
archive() ... 259
bounce() ... 260
deliver() ... 261
drop() ... 263
reprocess() ... 264
**7 Befehle für kryptographische Behandlung ... 265**
openPGP ... 265
pgp_encrypted() ... 265
Domänen basiert ... 266
decrypt_domain_pgp() ... 266
domain_pgp_keys_avail() ... 267
encrypt_domain_pgp() ... 268
Benutzer basiert ... 269
decrypt_pgp() ... 269
pgp_keys_avail() ... 270
encrypt_pgp() ... 271
S/MIME ... 272
smime_encrypted() ... 272
Domänen basiert ... 273
decrypt_domain_smime() ... 273
domain_smime_keys_avail() ... 274
encrypt_domain_smime() ... 275
Benutzer basiert ... 276
decrypt_smime() ... 276
smime_keys_avail() ... 277
encrypt_smime() ... 278
smime_signed() ... 279
validate_smime_sig() ... 280
delete_smime_sig() ... 281
sign_smime() ... 282
GINA ... 283
encrypt_webmail() ... 283
pack_mail() ... 284
unpack_mail() ... 284

© 2015 SEPPmail AG

webmail_keys_avail() ... 286
webmail_keys_gen() ... 287
**8 Befehle für LDAP (Zugriff auf externe Quellen) ... 288**
ldap_read ... **288**
ldap_compare() ... **290**
ldap_getcerts() ... **292**
ldap_getpgpkeys() ... **293**
**9 Befehle für Content Management ... 294**
iscalendar() ... **294**
isspam() ... **295**
vscan() ... **296**
**10 Vordefinierte Funktionen ... 297**
@ADDDISCLAIMER@ ... **297**
@ARCHIVE@ ... **297**
@CREATEGPGKEYS@ ... **297**
@CREATEUSER@ ... **297**
@CREATESEPPMAILACCOUNT@ ... **297**
@KEYSERVER@ ... **298**
@REMOVETAGS@ ... **298**
@REMOVELFMTAGS@ ... **298**
@REMOVETAGDECRYPTED@ ... **298**
@REMOVETAGSIGNED@ ... **299**
@REMOVETAGSIGNEDINVALID@ ... **299**
@TAGHEADERENCRYPTED@ ... **299**
@TRIGGERTEXT@ ... **300**
**11 Anwendungsbeispiele für das Regelwerk ... 301**
Bounce von E-Mails nicht authentifizierter Benutzer ... **301**
GINA-Verschlüsselung/Tagging zwischen Mandanten erzwingen ... **302**

© 2015 SEPPmail AG

# 1 Vorwort

Die SEPPmail AG behält sich vor, am Inhalt dieses Dokuments jederzeit und unangekündigt, Änderungen vorzunehmen. Sofern nicht anders vermerkt sind Namen und Daten von Personen oder Unternehmen, die in diesem Dokument als Anwendungsbeispiele verwendet werden, frei erfunden. Das Herstellen einer angemessenen Zahl von Kopien dieses Dokuments ist gestattet, jedoch nur für den internen Gebrauch. Zu anderen Zwecken darf dieses Dokument weder kopiert noch reproduziert werden; weder teilweise noch vollständig, nicht elektronisch, mechanisch oder auf irgendeine andere Weise, ausser mit ausdrücklicher, schriftlicher Genehmigung der SEPPmail AG.

Der Inhalt dieses Dokuments kann möglicherweise verändert worden sein, falls Sie es nicht direkt von der SEPPmail AG erhalten haben. Auch wenn dieses Dokument mit der grössten Sorgfalt angefertigt wurde, übernimmt die SEPPmail AG keine Verantwortung für etwaige Fehler oder Unvollständigkeiten. Das Benutzen dieses Dokuments beinhaltet die Zustimmung zu dessen Gebrauch ohne Mangelgewähr und ohne jegliche Garantien. Jeglicher Gebrauch der hier aufgeführten Informationen erfolgt auf eigenes Risiko.

PGP und Pretty Good Privacy sind gesetzlich geschützte Warenzeichen der PGP Corporation, gültig in den USA und anderen Ländern. Java und alle Java-basierten Marken sind Warenzeichen Oracle Corporation, gültig in den USA und anderen Ländern. UNIX ist ein eingetragenes Warenzeichen unter der Verfügung der X/Open Company, gültig in den USA und anderen Ländern. Microsoft, Internet Explorer, Windows, Windows NT, Windows 2000, Windows XP, Windows Vista, Windows 7, Windows 8 und Windows 10 sind entweder eingetragene Warenzeichen oder gesetzlich geschützte Warenzeichen der Microsoft Corporation, gültig in den USA und anderen Ländern. Netscape und Netscape Navigator sind gesetzlich geschützte Warenzeichen der Netscape Communications Corporation, gültig in den USA und anderen Ländern. Google Chrome sind gesetzlich geschützte Warenzeichen der Google Inc., gültig in den USA und anderen Ländern. Alle etwaigen anderen hier aufgeführten Warenzeichen sind Eigentum ihrer jeweiligen Besitzer und werden hier ohne die Absicht der Markenverletzung verwendet.

OpenBSD ist ein Betriebssystem, das unter dem Berkeley Copyright vertrieben wird (www.openbsd.org).
LibreSSL ist eine vom OpenBSD-Team von nicht benötigten Bestandteilen befreite Abspaltung von OpenSSL und wird unter der OpenBSD Lizenz vertrieben (www.libressl.org).
Der Apache Webserver und Apache Tomcat werden unter dem Apache Software Foundation Copyright entwickelt (www.apache.org).
OpenLDAP ist eine Implementierung des LDAP, die als freie Software unter der, BSD-Lizenz ähnlichen, OpenLDAP Public License veröffentlicht wird (www.openldap.org).
GnuPG ist Software, die unter der GNU Public License vertrieben wird (www.gnupg.org).
SpamAssassin ist ein Filterprogramm, mit dem unerwünschte E-Mails (Spam) automatisch aussortiert werden können und ist als freie Software unter den Bedingungen der Version 2 der Apache-Lizenz freigegeben (http://www.spamassasin.org).
ClamAV ist ein unter der GPL stehendes von der Sourcefire Inc. (http://www.sourcefire.com/) entwickeltes Virenschutzprogramm (http://www.clamav.net).

Hinweise auf kommerzielle Produkte, Verfahren oder Dienstleistungen, durch Nennung des Produkt- oder Herstellernamens oder auf beliebige andere Weise, kommen nicht notwendigerweise einer Billigung, Empfehlung oder Favorisierung durch die SEPPmail AG gleich.

Einfuhr, Ausfuhr und Benutzung dieser und anderer Verschlüsselungsprodukte sind möglicherweise gesetzlich eingeschränkt.

In diesem Dokument vom Verfasser geäusserte Ansichten und Meinungen drücken nicht notwendigerweise jene der SEPPmail AG aus und dürfen nicht zum Zweck der Werbung oder der Produktempfehlung benutzt werden. Verweise auf Internetadressen sind vor der Drucklegung gründlich geprüft worden. Aufgrund des ständigen Wandels der Internetinhalte kann die SEPPmail AG aber keine Garantie für das Vorhandensein und den Inhalt der angegebenen Quellen übernehmen. Sollten Sie in dieser Anleitung fehlerhafte Links finden, teilen Sie uns dies bitte unter Angabe des

© 2015 SEPPmail AG

betroffenen Links und der Versionsnummer dieser Anleitung an die Adresse info@seppmail.ch mit.
Druck: March 1015, CH-5432 Neuenhof

© 2015 SEPPmail AG

# 2 Einleitung

**Willkommen zur Secure E-Mail Lösung SEPPmail**

Das vorliegende Handbuch unterstützt bei der SEPPmail Installation und dient als Referenz der einzelnen Konfigurationsaspekte. Es ist in folgende Teile gegliedert:

| | |
|---|---|
| **Teil I** | **Vorwort** |
| **Teil II** | **Einführung** in das Produkt.<br>Allgemeine Informationen zu kryptographischen Verfahren sowie wichtige Produktmerkmale der SEPPmail Appliance. |
| **Teil III** | **Beschreibung** des Produkts<br>An dieser Stelle wird das komplette Produkt inklusive der Funktionsweise sowie aller Features detailliert beschrieben. |
| **Teil IV** | **Inbetriebnahme** des SEPPmail Secure E-Mail Gateways.<br>Dies beinhaltet das Integrieren der Appliance in das Netzwerk sowie das Anpassen der vorhandenen E-Mail- und Netzwerk-Umgebung. |
| **Teil V** | **Administrative Aufgaben**<br>Beschreibt die regelmässig anfallenden Aufgaben zur Wartung des SEPPmail-Systems |
| **Teil VI** | **Microsoft Outlook AddIn**<br>Beschreibt Einrichtung und Bedienung des zur Steuerung der Appliance kostenfrei zur Verfügung gestellte MS Outlook AddIn |
| **Teil VII** | **Referenz** der Menüpunkte.<br>Hier werden die Konfigurationsmöglichkeiten innerhalb der Menü-Struktur detailliert beschrieben. |
| **Teil VIII** | **Referenz** der Regelwerk Anweisungen.<br>Hier werden Befehle für individuelle Regelwerk Anweisungen erklärt, wie sie gegebenenfalls zur Integration in komplexe Infrastrukturen benötigt werden. |

© 2015 SEPPmail AG

## 2.1 Dokumentationsvereinbarungen

Um die Dokumentation übersichtlicher zu gestalten, werden unterschiedliche Schreibweisen und Symbole verwendet. Eine Übersicht der verwendeten Symbole und Schreibweisen für zum Beispiel Programmiercode, Menüpunkte oder Schaltflächen ist in der folgenden Tabelle dargestellt:

| | |
|---|---|
| | Hinweis auf mögliche Fehlerquellen oder Abschnitte in denen besondere Sorgfalt bei der Konfiguration notwendig ist. |
| | Wichtiger Hinweis |
| Kapitelverweis | Verweis auf ein Kapitel in dieser Dokumentation |
| Home | Menüpunkt |
| Sektion | Sektion |
| clusertid.txt | Spezielle Eingabefelder, Eingabewerte oder Ausgabewerte/Dateien |
| Create ruleset | Schaltfläche |
| ldap_compare(); | Programmiercode |

© 2015 SEPPmail AG

## 2.2 Sichere E-Mail-Kommunikation durch Verschlüsselung

Grundsätzlich unterscheidet man zwischen symmetrischer und asymmetrischer Verschlüsselung. Dabei hat jedes Verfahren seine Vor und Nachteile.

**Symmetrisch**
Bei der symmetrischen Verschlüsselung wird mit einem Schlüssel verschlüsselt. Der Kommunikationspartner muss für das Entschlüsseln im Besitz des gleichen Schlüssels sein. Das heisst jedoch, für jeden Kommunikationspartner muss ein eigener Schlüssel verwendet werden. Problematisch dabei ist der sichere Austausch der Schlüssel, sowie das Verwalten der Schlüssel bei vielen Kommunikationspartnern. Diese Art des Verschlüsselns ist wenig rechenintensiv und somit schnell und Ressourcen schonend.

**Asymetrisch**
Bei der asymmetrischen Verschlüsselung werden zwei Schlüssel verwendet, ein öffentlicher Teil (public key) und ein privater Teil (private key oder secret key). Dabei gleicht der öffentliche Schlüssel einem Vorhängeschloss, der private Schlüssel dem passenden Schlüssel zu diesem Schloss. Somit muss dem Absender eines zu verschlüsselnden Dokumentes muss nur der „public key“ des Empfängers bekannt sein. Nur der Empfänger mit dem dazu passenden „privaten Schlüssel“ wird in der Lage sein, das Dokument wieder zu entschlüsseln.
Somit kann der „public key“ ohne weitere Sicherheitsmassnamen an jeden beliebigen Kommunikationspartner gegeben werden und ist somit mehrfach verwendbar. Dieses Verfahren ist allerdings sehr rechenintensiv und deshalb langsam und Ressourcen raubend.

**Hybrid**
Mit dem hybriden Verfahren werden die Vorteile aus symmetrischer und asymmetrischer Verschlüsselung genutzt. So wird das zu verschlüsselnde Dokument Ressourcen schonend und schnell symmetrisch verschlüsselt. Der Austausch des symmetrischen Schlüssels erfolgt mittels asymetrischer Verschlüsselung. Aus diesem Grund hat sich dieses Verfahren für die Dokumentenverschlüsselung durchgesetzt.

Bei den nachfolgend beschriebenen Standardverfahren **S/MIME** und **openPGP** handelt es sich deshalb ebenfalls um hybride Verfahren.
SEPPmail setzt auf verschiedene standardisierte Verschlüsselungsverfahren und bietet dadurch höchste Sicherheit für unterschiedliche Kommunikationspartner. In diesem Abschnitt werden die Verfahren erläutert, die dabei zum Einsatz kommen.

Die Secure E-Mail-Gateway Appliance SEPPmail entschlüsselt eingehende E-Mails automatisch. Der Vorgang ist für den E-Mail-Empfänger komplett transparent. Er erhält seine E-Mails unverschlüsselt in seiner Mailbox und liest diese wie bisher, ohne Zusatzaufwand.

Eingehende E-Mails können mit einer digitalen Signatur versehen sein. Bestandteil dieser Signatur ist der öffentliche S/MIME Schlüssel (Zertifikat) des Absenders. Um den Verwaltungsaufwand zu minimieren, speichert die SEPPmail Appliance diese S/MIME Zertifikate nach erfolgreicher Prüfung automatisch, wodurch sie im Anschluss für das Verschlüsseln von E-Mails an die entsprechenden Kommunikationspartner bereit stehen.

Für den sicheren E-Mail-Versand wählt die SEPPmail-Appliance aus folgenden **5 Methoden** die für den Empfänger bestmögliche aus:

1. **S/MIME Benutzerverschlüsselung**

© 2015 SEPPmail AG

Sofern auf der SEPPmail-Appliance entsprechendes Schlüsselmaterial vorhanden ist, läuft die Verschlüsselung mittels S/MIME vollautomatisch ab. Für das Erlangen öffentlicher Schlüssel der Kommunikationspartner werden diese automatisch aus den S/MIME Signaturen eingehender E-Mails eingesammelt. Schlüsselpaare für interne Benutzer können auf der SEPPmail-Appliance selbst erstellt oder durch einen öffentlichen Zertifikatsanbieter ausgestellt werden. In beiden Fällen lassen sich die Zertifikate auch automatisiert erstellen. Die SEPPmail-Appliance unterstützt zu diesem Zweck verschiedene Schnittstellen zu öffentlichen Zertifikatsanbietern (CAs).

**2. openPGP Benutzerverschlüsselung**

openPGP funktioniert nach dem gleichen Grundprinzip wie S/MIME. Auch die openPGP-Schlüssel werden auf der SEPPmail-Appliance verwaltet und E-Mails entsprechend automatisch ver- und entschlüsselt, sofern das benötigte Schlüsselmaterial vorhanden ist. Im Gegensatz zu S/MIME werden die Schlüssel bei openPGP in der Regel immer selbst erzeugt. Dies liegt in der Tatsache begründet, dass openPGP im Gegensatz zu S/MIME nicht hierarchisch aufgebaut ist. Aus diesem Grund ist auch ein automatisiertes Einsammeln von öffentlichen Schlüsseln ist im Gegensatz zu S/MIME nicht möglich.

**3. E-Mail Domänen Verschlüsselung**

Die SEPPmail-Appliance bietet Ihnen die Möglichkeit, den E-Mail-Verkehr permanent zwischen mehreren E-Mail Domänen zu verschlüsseln. Auch hierfür kommen unterschiedliche Verfahren zum Einsatz

**a) S/MIME zwischen der SEPPmail Appliance und Secure E-Mail Gateways andererer Hersteller**

Dabei stellen sich die Kommunikationspartner gegenseitig jeweils Ihren öffentlichen S/MIME Domänen Schlüssel zur Verfügung. Da hierfür lediglich jeweils ein Zertifikat benötigt wird, und eine vorab Kommunikation der beiden Administratoren notwendig ist, kann in der Regel ein Self-Signed-Certificate verwendet werden.

**b) openPGP zwischen der SEPPmail Appliance und Secure E-Mail Gateways andererer Hersteller**

Dabei stellen sich die Kommunikationspartner gegenseitig jeweils Ihren öffentlichen openPGP Domänen Schlüssel zur Verfügung.

**c) per Managed Domänen Services - ohne jeglichen Konfigurationsaufwand - zwischen allen SEPPmail Appliances**

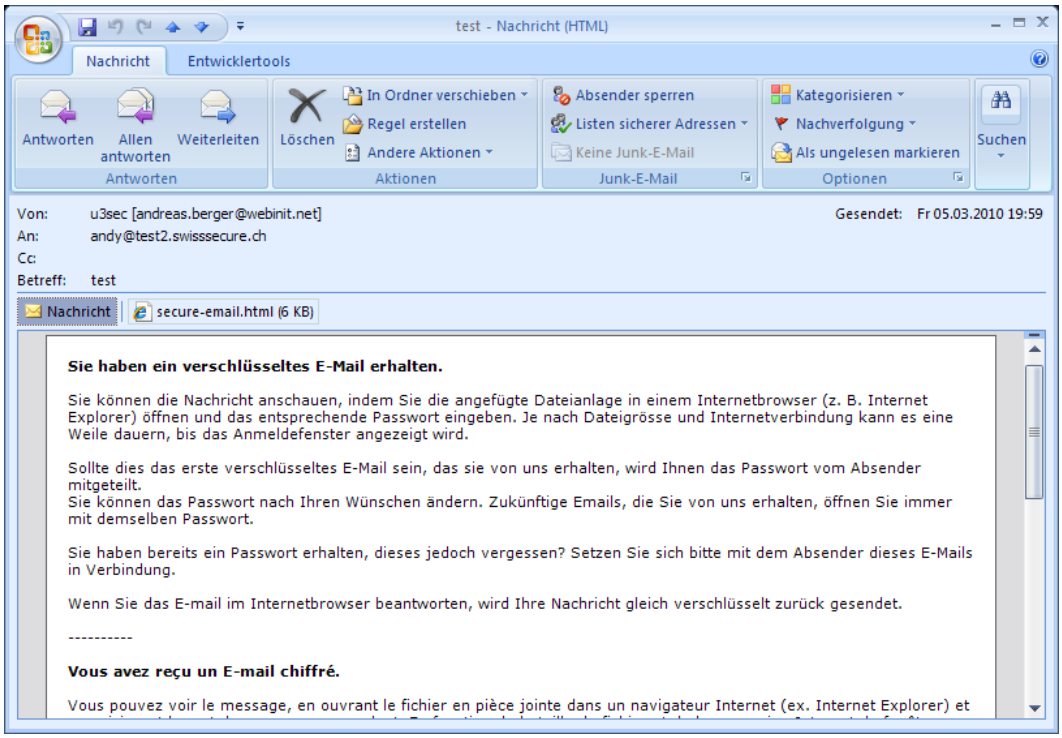
Die SEPPmail-Appliances tauschen über den Managed Domain Service vollautomatisiert die jeweils eigens hierfür durch die Appliance bereit gestellten öffentlichen S/MIME Domänen Schlüssel aus.
Somit wird grunsätzlich jeglicher E-Mail Verkehr zwischen SEPPmail-Appliances automatisch ver- und entschlüsselt.

© 2015 SEPPmail AG

## 4. GINA-Technologie

Bei der GINA-Verschlüsselungstechnologie handelt es sich um ein patentiertes Verfahren. Dabei werden E-Mails nicht bis zum Abholen durch den Empfänger zwischengespeichert, wie es bei anderen Webmail Verfahren üblich ist, sondern vollständig verschlüsselt an den Empfänger ausgeliefert. E-Mails sind bei diesem Verfahren vor Phishing-Attacken geschützt, denn neben dem Kennwort ist für den erfolgreichen Zugriff auch die verschlüsselte E-Mail selbst aus dem Postfach des Empfängers erforderlich.

Eine GINA-Nachricht enthält die komplette, ursprünglich unverschlüsselte Nachricht - inklusive Anhänge - in verschlüsselter Form als HTML-Dateianlage. Der Empfänger ruft die Nachricht ab, indem er die verschlüsselte Dateianlage im lokalen Webbrowser öffnet. Diese wird dann über eine sichere SSL-Verbindung (HTTPS) an die SEPPmail-Appliance des Absenders übertragen und dort nach Eingabe eines Benutzerkennworts entschlüsselt und angezeigt. Durch die Kennworteingabe wird die Identität des Empfängers bei jedem Abruf geprüft. Im Gegensatz zum herkömmlichen E-Mail-Versand können E-Mail-Zustellungen aufgrund der korrekten Authentifizierung des Empfängers nachgewiesen werden. Die nachfolgende Abbildung zeigt ein Beispiel einer GINA-Nachricht.


test - Nachricht (HTML)
Nachricht
Entwicklertools
Antworten
Allen antworten
Weiterleiten
Antworten
Löschen
In Ordner verschieben
Regel erstellen
Andere Aktionen
Aktionen
Absender sperren
Listen sicherer Adressen
Keine Junk-E-Mail
Junk-E-Mail
Kategorisieren
Nachverfolgung
Als ungelesen markieren
Optionen
Suchen
Von: u3sec [andreas.berger@webinit.net]
Gesendet: Fr 05.03.2010 19:59
An: andy@test2.swisssecure.ch
Cc:
Betreff: test
Nachricht
secure-email.html (6 KB)
Sie haben ein verschlüsseltes E-Mail erhalten.
Sie können die Nachricht anschauen, indem Sie die angefügte Dateianlage in einem Internetbrowser (z. B. Internet Explorer) öffnen und das entsprechende Passwort eingeben. Je nach Dateigrösse und Internetverbindung kann es eine Weile dauern, bis das Anmeldefenster angezeigt wird.
Sollte dies das erste verschlüsseltes E-Mail sein, das sie von uns erhalten, wird Ihnen das Passwort vom Absender mitgeteilt.
Sie können das Passwort nach Ihren Wünschen ändern. Zukünftige Emails, die Sie von uns erhalten, öffnen Sie immer mit demselben Passwort.
Sie haben bereits ein Passwort erhalten, dieses jedoch vergessen? Setzen Sie sich bitte mit dem Absender dieses E-Mails in Verbindung.
Wenn Sie das E-mail im Internetbrowser beantworten, wird Ihre Nachricht gleich verschlüsselt zurück gesendet.
---
Vous avez reçu un E-mail chiffré.
Vous pouvez voir le message, en ouvrant le fichier en pièce jointe dans un navigateur Internet (ex. Internet Explorer) et

**Beispiel einer GINA-Nachricht**

## 5. TLS/SSL Transportverschlüsselung

TLS/SSL bietet eine zusätzliche Sicherheit und ergänzt die bisher beschriebenen Verschlüsselungsmethoden. Die Kommunikation zwischen der SEPPmail-Appliance und anderen E-Mail Servern wird in der Standardkonfiguration immer über einen TLS/SSL gesicherten Kanal aufgebaut, sofern die Gegenstelle dies unterstützt.

© 2015 SEPPmail AG

## 2.3 Digitale E-Mail-Signaturen

Beim Einsatz digitaler E-Mail-Signaturen wird die verbindliche E-Mail-Kommunikation gewährleistet, indem die Authentizität einer Nachricht verifiziert werden kann. Somit wird sichergestellt, dass eine Nachricht unverändert beim Empfänger eintrifft und der angezeigte Absender auch dem tatsächlichen Absender entspricht.

Das Secure E-Mail-Gateway SEPPmail kann E-Mails entweder mit Benutzer- oder mit Firmen-Zertifikaten signieren. Die beiden Verfahren werden im Folgenden kurz erläutert:

**Digitale E-Mail-Signatur mit einem Benutzerzertifikat**

Das Signieren von E-Mails mit einem S/MIME-Benutzerzertifikat erlaubt dem Empfänger die Authentizität der E-Mail mit seinem E-Mail-Client zu prüfen. Damit wird sichergestellt, dass der Absender authentisch ist und die E-Mail während und nach dem Versand nicht verändert wurde. Bei dieser Methode wird für jeden E-Mail-Absender ein eigenes S/MIME-Zertifikat benötigt.

In der Regel können nur Zertifikate offizieller Zertifikatsanbieter (Trusted CA) automatisiert vom Empfänger geprüft werden. Aus diesem Grund wird dringend das Verwenden solcher offiziellen Zertifikate empfohlen. Die SEPPmail-Appliance bietet mit ihren integrierten CA-Connectoren die Möglichkeit den Bezug von Zertifikaten einiger offizieller Zertifizierungsstellen zu automatisieren.

Alternativ ist das Signieren von E-Mails auch im E-Mail-Client des jeweiligen Absenders möglich. Das SEPPmail Secure E-Mail-Gateway wird diese E-Mails dann nur noch verschlüsseln. Da sich viele S/MIME-Zertifikate zum Signieren und Verschlüsseln von E-Mails eignen, kann es sinnvoll sein, solche Zertifikate zusätzlich auf der SEPPmail-Appliance zu installieren. Dadurch können E-Mails bereits an der SEPPmail-Appliance mit den entsprechenden Zertifikaten automatisch entschlüsselt und somit zum Beispiel zentral archiviert oder auf Viren geprüft werden.

**Digitale E-Mail-Signatur mit einem Firmenzertifikat**

Das Signieren von E-Mails mit einem S/MIME-Firmenzertifikat erfüllt auf Unternehmensebene denselben Zweck wie das Signieren mit einem S/MIME-Benutzerzertifikat auf Personenebene. Bei dieser Variante wird nur ein einziges Zertifikat für das Unternehmen benötigt. Da S/MIME-Zertifikate grundsätzlich jedoch nur für eine E-Mail-Absenderadresse gültig sind, erhalten alle ausgehenden E-Mails den gleichen (technischen) Absender. Das heisst alle E-Mails des Unternehmens - egal wer im Unternehmen der Absender ist - erscheinen beim Empfänger mit derselben E-Mail-Adresse. Daraus resultieren einige Probleme:

- Zwar wird beim Empfänger der korrekte Benutzername angezeigt, jedoch wird ein automatisches Erfassen von Kontakten und zugehörigen E-Mail-Adressen nicht mehr wie erwartet funktionieren.
- Aufgrund der Häufigkeit, mit welcher diese eine Absenderadresse bei Einsatz dieser Technologie verwendet wird, besteht eine hohe Wahrscheinlichkeit, dass diese fälschlicherweise als SPAM eingestuft wird.
  Das hätte zur Folge, dass bei den meisten Empfängern alle E-Mails des Unternehmens abgewiesen würden.
- Non Delivery Reports (NDR) also Informations-Mails welche bei Nicht-Zustellbarkeit erzeugt werden, werden nicht an den ursprünglichen, sondern an den technischen Absender gesendet
- ...

Fazit:
Diese Art der Signatur ist im produktiven Umfeld absolut nicht zu empfehlen, da über kurz oder lang massive Support Aufwände generiert werden!

© 2015 SEPPmail AG

## 2.4 Zentrale Firmen E-Mail Fussnote

Das SEPPmail Secure E-Mail-Gateway kann Ihre E-Mails mit Firmen E-Mail-Disclaimer ergänzen. Disclaimer werden sowohl im Text- wie auch HTML-Format unterstützt.

Zentrale Firmendisclaimer, können verwendet werden um einheitlichen Text wie zum Beispiel Adresse und Firmeninhaber an E-Mails anzuhängen.

**Beispiel im Textformat:**

```
Firma AG - Musterstrasse 1, 1234 Musterstadt - www.meinefirma.ch
```

## 2.5 Kompatibilität zu anderen Secure E-Mail Systemen

Aufgrund des Verwendens genormter Techniken und Protokolle lässt sich SEPPmail transparent in jede E-Mail-Infrastruktur integrieren. Alle anerkannten und sicheren Standard-Verschlüsselungstechniken sind implementiert. Die Kompatibilität zu den gängigen E-Mail-Systemen ist damit sichergestellt und die Installation zusätzlicher Softwarekomponenten entfällt.

Für Empfänger, die keine S/MIME Zertifikate oder openPGP Schlüssel besitzen, kann die GINA-Technologie für das sichere Übertragen von E-Mails genutzt werden.

## 2.6 Remote-Administration mittels Web-Portal

Sämtliche Verwaltungsmöglichkeiten des SEPPmail Secure E-Mail-Gateways stehen über eine Webbrowser basierte Konfigurationsoberfläche zur Verfügung. Die Verbindung zwischen Webbrowser und dem SEPPmail Secure E-Mail-Gateway ist zusätzlich SSL verschlüsselt (HTTPS).

© 2015 SEPPmail AG

# 3 Die SEPPmail-Appliance

## 3.1 SEPPmail AG (Hersteller)

Das in der Schweiz ansässige, international tätige und inhabergeführte Unternehmen SEPPmail ist Hersteller im Bereich „Secure Messaging“. Dessen patentierte, mehrfach prämierte Technologie für den spontanen sicheren E-Mail-Verkehr (GINA) verschlüsselt elektronische Nachrichten und versieht diese auf Wunsch mit einer digitalen Signatur. Die Secure E-Mail-Lösungen sind weltweilt erhältlich und leisten einen nachhaltigen Beitrag zur sicheren Kommunikation mittels elektronischer Post. Dadurch maximiert SEPPmail die Kommunikationssicherheit von hunderttausenden von Benutzern. Das Unternehmen wurde 2001 gegründet und verfügt demnach über eine mehr als zehnjährige Erfahrung im sicheren Versenden digitaler Nachrichten.

Die Produktphilosophie gründet sich auf zwei Hauptmerkmale: ein Höchstmass an Sicherheit, in Kombination mit hohen Benutzerkomfort. Zu letzterem zählen insbesondere einen hochverfügbaren Betrieb mit hoher Stabilität und geringen Administrationsaufwände.

SEPPmail AG hat mit seinem CEO, Herrn Stefan Klein, den „Erfinder“ dieser Lösung on board, der seit 2001 die Entwicklung dieses Produktes betreut und begleitet. Dabei stellte er sicher, dass die Produktphilosophie über all die Jahre beibehalten wurde. So reifte das Produkt mit den Kundenanforderungen, wobei die individuellen Anforderungen immer dem Gesamtprodukt beigefügt und somit allen Kunden zugängig wird.

SEPPmail AG
Industriestrasse 7
CH-5432 Neuenhof

http://www.SEPPmail.ch

© 2015 SEPPmail AG

## 3.2 Vorstellung und Verfahren

### 3.2.1 Produktphilosophie

Die Produktphilosophie gründet sich auf zwei Hauptmerkmale: ein Höchstmass an Sicherheit, in Kombination mit hohem Benutzerkomfort. Zu letzterem zählen insbesondere ein stabiler Betrieb und möglichst geringe Administrationsaufwände.

Das Produkt unterstützt alle am Markt befindlichen Standard-Technologien (siehe S/MIME (X.509) 20, openPGP 20, TLS 21) für das Absichern des E-Mail Verkehrs mittels Verschlüsselung und Signatur.

Darüber hinaus hat SEPPmail ein Verfahren entwickelt und patentiert, welches erlaubt, einem gänzlich „unbekannten“ Empfänger spontan eine verschlüsselte E-Mail zu senden. Der Empfänger benötigt für das Entschlüsseln sowie dem sicheren Antworten ausschliesslich Standardkomponenten, wie einen beliebigen E-Mail Client (dies kann auch ein Webmail Client sein), einen beliebigen Browser und Zugang zum Internet, unabhängig vom Endgerät. Wir nennen diese Technologie GINA (siehe GINA Webmail 23).

Ein mit der Lösung ausgeliefertes Standard-Ruleset (siehe Zentrales Regelwerk 38) ermöglicht das 100%ige Verschlüsseln aller als vertraulich gekennzeichneten, zu versendenden E-Mails. Dabei wird über das Ruleset die für den jeweiligen Empfänger beste Verschlüsselungstechnologie ausgewählt. Beginnend mit der Prüfung, ob ein beglaubigter öffentlicher S/MIME Schlüssel des Empfängers für das Verschlüsseln zur Verfügung steht, kaskadiert das System über openPGP, Domänen Verschlüsselung runter bis zur „GINA“ Technologie (siehe Verschlüsselungshierarchie 22). Diese kommt nur dann zum Einsatz, falls kein geeignetes Schlüsselmaterial des Empfängers vorliegt oder vom Versender ganz bewusst - für den Erhalt einer verbindlichen Lesebestätigung - gewählt wird.

SEPPmail besteht aus nur einem Hauptprodukt, welches allen Kunden zur Verfügung gestellt wird. Einzelne Features, welche von Kunden gewünscht werden und in das Gesamtkonzept in punkto Sicherheit und Benutzerkomfort passen, werden kostenfrei von SEPPmail implementiert und kommen somit allen Kunden zu Gute.

Die Lösung wird als komplette, auf openBSD basierende Firmware geliefert. Damit entfällt das aufwendige Installieren und Warten von Einzelkomponenten, wie zum Beispiel Datenbanken oder Funktionsmodulen. Das Update erfolgt auf Knopfdruck für das gesamte System.

#### 3.2.1.1 Fünf generische Prinzipien

1. **Angemessenes Absichern der Geschäftsdaten**
   Das Absichern wird durch den Einsatz bewährter Verschlüsselungstechnologien (S/MIME, openPGP, TLS und GINA) sowie durch eine gehärtete Appliance garantiert.

2. **Kosteneffizienter Betrieb**
   Kosteneffizienz wird durch den Appliance – Ansatz, einen hohen Automatisierungs- und Standardisierungsgrad und insbesondere einen sehr niedrigen Support Aufwand der GINA-Technologie im Vergleich zu anderen Methoden (PDF oder Webmailer) erreicht.

3. **Hohe Anzahl von Kunden und Geschäftspartnern erreichbar**
   Den besten Beweis für die „Massentauglichkeit“ der patentiertenGINA-Technologie erbringt der Dienst „Incamail“ der Schweizerischen Post. Uns ist kein Projekt bekannt bei der mit alternativen Methoden auch nur annähernd so viele Kunden bedient bzw. so viele E-Mails verschlüsselt werden. Als stiller Champion stellt sich mehr und mehr die Domänen Verschlüsselung heraus (siehe Gateway-to-Gateway (Domänen-) Verschlüsselung 21). Ein nicht zu unterschätzender Anteil der E-Mail Kommunikation zwischen Unternehmen wird mittlerweile mittels der völlig transparenten Domänen Verschlüsselung gesichert.

© 2015 SEPPmail AG

4. **Hoher Grad von Akzeptanz**
   Auch hier möchten wir wieder auf die GINA-Technologie verweisen. Damit ist eine einfache Zwei-Weg–Kommunikation möglich. Separate Kommunikationskanäle (PDF zum Kunden – Rückweg über ein Webportal) sind nicht nötig.

5. **Erfüllen der geschäftlichen und rechtlichen Rahmenbedingungen**
   Bei der GINA-Technologie werden E-Mails generell vollständig verschlüsselt ausgeliefert. Damit gelangt die E-Mail in den 100%igen Einflussbereich des Empfängers. Rechtliche Probleme betreffend vollständiger Auslieferung von E-Mails (Wie dies bei einem „normalen“ sicheren Webmail der Fall wäre) bestehen somit nicht.

© 2015 SEPPmail AG

## 3.2.2 Verschlüsselungstechnologien

### 3.2.2.1 S/MIME (X.509)

Da die SEPPmail-Appliance in der Regel im vollen E-Mail Strom steht (siehe auch Architekturen -> Im vollen E-Mail Strom 39), lernt diese automatisch alle S/MIME Public Keys, die über E-Mail-Signaturen eingeliefert werden. Sind diese von einer der SEPPmail bekannten CA (Certificate Authority) ausgestellt, können diese geprüft und akzeptiert werden (vollautomatischer Vorgang). Ist die CA nicht bekannt, wird dies bemerkt und dem Administrator zur Prüfung vorgelegt (halbautomatischer Vorgang). Erfahrungsgemäss nimmt dieser Aufwand nach einer Einschwingphase des Systems merklich ab, da die meisten Signaturen gelernt und Root-Zertifikate geprüft wurden. Wird eine als vertraulich gekennzeichnete E-Mail an einen externen Empfänger versendet, prüft das System erstrangig, ob ein freigegebener S/MIME Public Key des Empfängers existiert. Die E-Mail wird transparent verschlüsselt und versendet.

Wenn ein intelligentes E-Mail Routing – System beim Kunden vorhanden ist welches signierte und / oder verschlüsselte E-Mails erkennen kann, so können auch gezielt nur die nötigen E-Mails über die Appliance empfangen werden. Die Appliance muss dann nicht in den vollen E-Mail Strom integriert werden.

#### 3.2.2.1.1 Managed PKI

Die SEPPmail Appliance hat ein vollständiges PKI-System eingebaut und verwaltet User Schlüssel bzw. Zertifikate zentral im System. E-Mail Zertifikate können von beliebigen CAs eingespielt werden. Zu den wichtigsten CAs hat SEPPmail jedoch Konnektoren geschrieben:

- SwissSign
- S-Trust (DSV)
- D-Trust (Bundesdruckerei)
- A-Trust

Über diesen Konnektor werden die Zertifikate für die User automatisch erstellt und der Certificate Signing Request (CSR) automatisch an die jeweilige CA übermittelt. In der Appliance werden diese den Usern zugeordnet und zur Signatur herangezogen.

Der Bezug von Zertifikaten für die E-Mail-Konten ist daher flexibel und individuell konfigurierbar.

Bei Anlage eines neuen Benutzers – dies kann wahlweise automatisch zum Beispiel durch Anfordern von Verschlüsselung oder Signatur, oder manuell erfolgen - kann gewählt werden, ob ein E-Mail Zertifikat automatisch ausgestellt werden soll. Dieses kann dann von der internen (Sub-)CA oder über die MPKI Schnittstelle bezogen werden. Bei Bedarf sind auch beide Varianten parallel möglich.

Wird das Zertifikat über die MPKI bezogen, so wird das Schlüsselpaar auf der SEPPmail Appliance generiert und nur der öffentliche Schlüssel zum Signieren an die Trustet CA übermittelt. Der sensible private Schlüssel verlässt zu keiner Zeit die Appliance und liegt dort – wie das gesamte Schlüsselmaterial – in einem gesicherten Bereich ab.

Auch das Erneuern der Zertifikate ist vollautomatisiert möglich. Der Zeitraum, wieviele Tage vor Ablauf des alten Zertifikates ein neues generiert werden soll ist dabei frei wählbar.

### 3.2.2.2 OpenPGP

Zur nachteiligen Natur von openPGP Schlüsseln gehört, dass diese - bevor sie für das Verschlüsseln herangezogen werden können - zuerst validiert werden müssen. Somit ist ein automatisiertes Prüfen nicht möglich (Prinzip: web of trust). Theoretisch müsste daher bei jedem zu importierenden öffentlichen openPGP Schlüssel über einen separaten Kanal der Fingerabdruck (Hash) des Schlüssels geprüft werden. SEPPmail hat ein "umgedrehtes" Verfahren realisiert: Wenn der Empfänger eine GINA-E-Mail (siehe GINA Webmail 23) erhält, so wird ihm darüber auch die Möglichkeit gegeben, den eigenen öffentlichen Schlüssel - egal ob openPGP oder S/MIME - auf die

© 2015 SEPPmail AG

Appliance hochzuladen. Durch die vorangegangene Authentifizierung des Empfängers durch E-Mail und Initial-Passwort am GINA-Web-Interface ist kein zusätzliches Validieren durch die Administration oder den Sender notwendig.

#### 3.2.2.3 LDAP Key-Lookup für S/MIME und OpenPGP

Eine LDAP Lookup Funktionalität ist in der Lösung integriert. Beim Erfassen von Key Servern ist allerdings auf die Qualität dieser zu achten. Häufig wird über "öffentliche" Key Server „totes“ Schlüsselmaterial verbreitet. Verwendet der Absender dieses Material, so kann der Empfänger die damit verschlüsselte E-Mail unter Umständen - mangels privatem Schlüssel - nicht lesen.

#### 3.2.2.4 TLS

SEPPmail nutzt im Normalfall „opportunistisches TLS“, sprich TLS (mit der jeweils höchstmöglichen Verschlüsselung) wird benutzt, wenn dies vom gegenüberliegenden E-Mail Server bzw. MTA (Mail Transfer Agent) unterstützt und angeboten wird.
Zusätzlich können für einzelne E-Mail Domänen und/oder E-Mail Server spezifisch TLS – Level erfasst werden. (mit den Postfix – typischen Stufen „may“, „verify“, „secure“, „fingerprint“ und bald auch „dane“).
TLS „gezielt“ als Ersatz für eine Verschlüsselung von E-Mails zu verwenden erscheint schwierig, und zwar primär aus folgenden Gründen:

- Bei Verwenden von TLS wird maximal bis zum nächsten MTA verschlüsselt. Da immer mehr Firmen Cloud–Dienste für das Filtern von Spam E-Mails verwenden, reicht dies normalerweise nicht
- Eigentlich darf TLS nur bei Einsatz der Sicherheitsstufe „Fingerprint“ oder „DANE“ als einigermassen sicher betrachtet werden. Alle anderen Sicherheitsstufen sind - zum Beispiel durch DNS Spoofing - aushebelbar
- Das Verwalten von TLS Verbindungen erzeugt hohen Administrationsaufwand

Trotz dieser Nachteile erfreut sich TLS in letzter Zeit steigender Beliebtheit – wahrscheinlich weil TLS als „kleinster gemeinsamer Nenner“ auf praktisch jedem MTA verfügbar ist. SEPPmail plant deshalb auch, den TLS – Support zu erweitern.

### 3.2.3 Gateway-to-Gateway (Domänen-) Verschlüsselung

Eine Grundfunktionalität aller SEPPmail-Appliances ist der „Managed Domain Service“. Dieser Service stellt sicher, dass jeder SEPPmail-Appliance jeweils die öffentlichen Domänen Schlüssel aller anderen SEPPmail-Appliances zur Verfügung stehen. Somit kann zwischen den teilnehmenden Kunden das vollautomatische und transparente Verschlüsseln des gesamten E-Mail Verkehrs von Gateway zu Gateway (Domänen Verschlüsselung) gewährleistet werden.

Durch den manuellen Austausch der öffentlichen Domänen Schlüssel lässt sich die Domänen Verschlüsselung auch mit Gateways anderer Hersteller realisieren.

Die beiden Verschlüsselungstechnologien TLS und Gateway-to-Gateway sind Bestandteil der SEPPmail-Appliance Grundlizenz und müssen nicht per User lizensiert werden.

© 2015 SEPPmail AG

### 3.2.4 Verschlüsselungshierarchie

Das von SEPPmail initial zur Verfügung gestellte Standard-Ruleset gibt für E-Mails die folgende Vorgehensweise vor:
Wurde eine E-Mail als zu verschlüsselnd markiert, so wird diese „best effort“ behandelt. Dabei wird nach folgender Wertigkeit vorgegangen:

1. Geprüftes S/MIME Zertifikat des Empfängers
2. Geprüfter öffentlicher openPGP Schlüssel des Empfängers
3. Geprüftes S/MIME Domänen Zertifikat des Empfängers
4. Geprüfte öffentlicher openPGP Domänen Schlüssel des Empfängers

   Sollte aufgrund fehlenden Schlüsselmaterials des Empfängers keines der vorangegangenen (Standard-)Verfahren verfügbar sein, so wird

5. GINA mit hinterlegtem Empfängerpasswort
6. GINA mit Initialpasswort

Es gilt zu beachten, dass die Verschlüsselungsverfahren der Punkte 3. und 4. auch bei nicht als zu verschlüsselnd markierten E-Mails zum Einsatz kommt, sofern diese Verfahren verfügbar sind.

Standard Verschlüsselungsmerkmale sind Betreffzeilen-Schlüsselworte, Sensitivity Parameter (Vertraulichkeitsmarkierung) sowie spezielle x-header.
Optional können auch zum Beispiel LDAP Abfragen als Merkmale herangezogen werden, wie etwa Microsoft Active Directory (AD) Benutzergruppen.

Sollte eine andere Reihenfolge, oder ein anderer Vorgang gewünscht werden, kann jederzeit das Ruleset entsprechend angepasst werden. Damit können gewünschte Standardisierungen im Umgang mit E-Mails an vorbestimmte Adressen oder Domänen so voreingestellt werden, dass diese Regelungen unabhängig von den Nutzeraktionen immer ziehen.

Darüber hinaus kann das Ruleset der Appliance bei Bedarf durch das eigens dafür bereit gestellte AddIn (siehe **MS-Outlook AddIn** 35) bzw. Betreffzeilen-Schlüsselworte übersteuert werden. Wobei diese Befehlswörter in der Regel vom Kunden vorgegeben und angepasst werden können.

Folgende Befehlswörter sind in der Standardinstallation vorgegeben:

| | |
|---|---|
| [plain] | E-Mail mit diesem Kennzeichen durchlaufen nicht das Ruleset und werden somit cryptographisch unbehandelt versendet |
| [confidential] | Anfordern der Verschlüsselung |
| [priv] | E-Mail mit diesem Kennzeichen werden mittels GINA-Technologie verschlüsselt (Stichwort Lesebestätigung) |
| [emptypw] | Die Notwendigkeit der Eingabe eines Initialpasswortes bei GINA-E-Mails wird unterdrückt (Sicherheitstechnisch bedenklich) |
| [SMS:<Mobilfunknummer>] | Mobilfunknummer zur Übertragung des Initialpasswortes einer GINA-E-Mail* |
| [noenc] | Verschlüsseln wird unterdrückt, sofern dies als Standard im Ruleset definiert wurde |
| [sign] | Anfordern der Signierung |
| [nosign] | Signieren wird unterdrückt, sofern dies als Standard im Ruleset definiert wurde |
| [lfm] | Aktiviert das Large File Management, unabhängig der E-Mail Grösse* |
| [lfm:nocrypt] | Der Empfänger Einer LFM Mail muss sich für das Abholen des "Large Files" nicht authentifizieren* |

**(*Funktionen, welche Zusatzllizenzen erfordern)**

Diese Schlüsselworte stehen natürlich nur dann zur Verfügung, wenn die zugehörigen Funktionen vom Administrator im Ruleset auch aktiviert wurden.

© 2015 SEPPmail AG

### 3.2.5 GINA Webmail

SEPPmail verfügt über eine patentierte Technologie zur Unterstützung von Benutzern ohne Secure E-Mail Infrastruktur. Diese Technologie benötigt lediglich einen Web-Browser und die Möglichkeit E-Mails zu empfangen, also Internetzugang. **Weitere Anforderungen an die Infrastruktur des Benutzers bestehen nicht.**

Diese Technologie bietet im Vergleich zu anderen auf dem Markt verfügbaren Lösungen für die sichere E-Mail Kommunikation mit beliebigen Partnern wichtige Vorteile:

| | Normales " secure Webmail" | PDF-Verschlüsselung | Selbstextrahierendes Archiv | Spezieller Client | Ausstellen eigener S/MIME - Zertifikate | GINA |
|---|---|---|---|---|---|---|
| Keine Speicherung ausgehender E-Mails | | | | | | ✓ |
| Phishing-Resistent | | | | | | ✓ |
| Resistent gegen Brute Force – Attacken | | | | | | ✓ |
| „Eingeschriebenes E-Mail" möglich | | | | | | ✓ |
| Keine Installation beim Empfänger | | | | | | ✓ |
| Auf den gängigen Plattformen lesbar | | | | | | ✓ |
| "Two-Factor Authentication" | | | | | | ✓ |

**a) Schritt 1: Sender - E-Mail verfassen**
Der Sender verfasst in seinem Standard E-Mail Client eine E-Mail und klassifiziert diese als vertraulich, indem er diese entweder

- mit den E-Mail Client Boardmitteln (1) als „vertraulich“ markiert.
- Er kann auch im Betreff ein frei definierbares, aber unternehmensweit vereinbartes Befehlswort

© 2015 SEPPmail AG

zum Beispiel (2) „[secure]“ einsetzen. Diese Methode greift auch für sogenannte System-User (= maschinelle Ansteuerung).

- oder er verwendet das kostenlose Outlook AddIn von SEPPmail (3) [Abb.1].

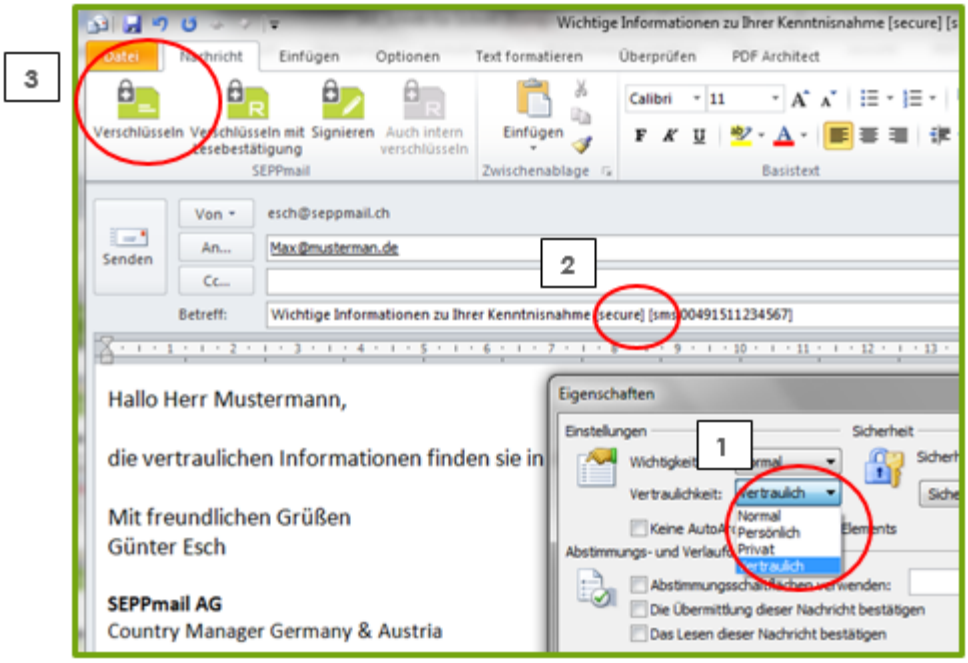



Abb. 1

Dabei kann er wählen zwischen:

a) „Verschlüsseln“ (Bezeichnung kann angepasst werden): Dabei wird die E-Mail am System mit den für den/die Empfänger zur Verfügung stehenden Technologien im „Best Effort“ Verfahren verschlüsselt und versendet.

b) „Verschlüsseln mit Lesebestätigung“ (Bezeichnung kann angepasst werden): Dabei wird immer zwingend die GINA-Technologie angezogen, denn nur dadurch kann eine Rückmeldung des Systems zum Zeitpunkt des aktiven Lesens der versendeten E-Mail sichergestellt werden. Diese Lesebestätigung ist vom externen Empfänger nicht abzuwählen.

Sollte dieses Verfahren der Kundenanforderung nicht entsprechen, kann das AddIn auch entsprechend angepasst werden. Das AddIn ist Standardmässig in den Sprachen Deutsch und Englisch verfügbar: Bei Bedarf können zusätzliche Sprachen realisiert werden. **Danach wird die E-Mail versendet**.

**b) Schritt 2: Sender - Verschlüsseln und Initialpasswort**

Die als vertraulich markierte E-Mail wandert durch den E-Mail Server und passiert danach die SEPPmail. Die Appliance erkennt, dass diese E-Mail zu verschlüsseln ist und leitet den unter A 2.2.5. beschrieben Vorgang zur Verschlüsselung ein. Sie sieht also nach, ob der oder die Empfänger schon bekannt sind. Sollten diese schon einmal eine S/MIME signierte E-Mail an einen beliebigen Mitarbeiter geschickt haben, oder haben sich schon einmal via GINA-Portal registriert bzw. ein eigenes S/MIME Zertifikat oder einen eigenen openPGP Key hochgeladen, dann wird Die E-Mail damit verschlüsselt.

**Wenn für den/die Empfänger keine Schlüssel hinterlegt sind, oder diese gänzlich „unbekannt“ sind, kommt die patentierte** GINA **Technologie von SEPPmail zum Einsatz.**

© 2015 SEPPmail AG

Bei dieser wird zuerst ein AES256 Key erzeugt, die vertrauliche E-Mail damit symmetrisch verschlüsselt und als HTML-Anhang an eine Standard-E-Mail beigefügt. Die E-Mail wird immer **vollständig ausgeliefert**. Auf der Appliance wird ausser den Empfängerdaten nichts zwischengespeichert. Beim erwähnten Anhang wird komplett auf aktiven Inhalt (wie zum Beispiel JavaScript) verzichtet. Es wir nur „plain HTML“ verwendet.

Der Key für den Empfänger bleibt dauerhaft auf der Appliance und wird für die erste, wie für alle anderen GINA-Mails zum Ver- und Entschlüsseln für diese Empfangsadresse verwendet.

Ein Initialpasswort wird erstellt und per E-Mail dem Sender zur Übermittlung an den Empfänger (per SMS (Abb.2), Telefon oder Fax) zugestellt.

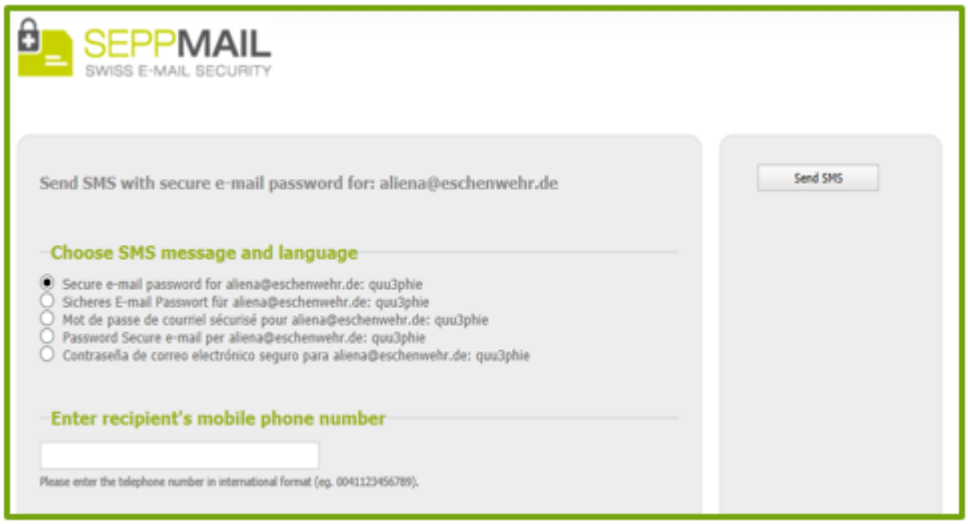

SEPPMAIL
SWISS E-MAIL SECURITY
Send SMS with secure e-mail password for: aliena@eschenwehr.de
Send SMS
Choose SMS message and language
Secure e-mail password for aliena@eschenwehr.de: quu3phie
Sicheres E-mail Passwort für aliena@eschenwehr.de: quu3phie
Mot de passe de courriel sécurisé pour aliena@eschenwehr.de: quu3phie
Password Secure e-mail per aliena@eschenwehr.de: quu3phie
Contrasella de correo electrónico seguro para aliena@eschenwehr.de: quu3phie
Enter recipient's mobile phone number
Please enter the telephone number in international format (eg. 0041123456789).

Abb 2

Die für den Anschluss an einen SMS Provider oder System notwendigen Schnittstellen sind in der Lösung eingebaut und konfigurierbar.

**c) Schritt 3: Empfänger – Anmelden und einmaliges Registrieren**

Der Empfänger öffnet den HTML-Anhang und wird zur Eingabe seines Initialpasswortes aufgefordert (Abb. 3). Dabei kann er auch seine gewünschte Sprache festlegen.
Anschliessend erfolgt eine **einmalige** Registrierung am System. Ein eigenes Passwort wird vergeben, sowie eine Sicherheitsfrage + Antwort festgelegt, um ein Zurücksetzen seines Passworts zu ermöglichen (Abb. 4) Optional kann eine Mobilfunknummer für den automatisierten SMS-Passwort-Versand eingegeben werden.

Beim nächsten Lesen der E-Mail, oder bei einer neuen vertraulichen E-Mail, wird nur noch das eigene Passwort eingeben (Abb. 3).

© 2015 SEPPmail AG

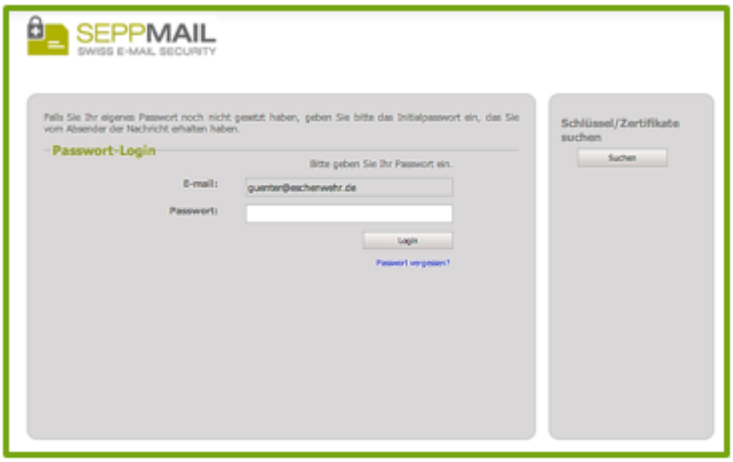



Abb. 3

Abb. 4

**d) Schritt 4: Empfänger - Lesen und sicher Antworten**

Danach wird die entschlüsselte E-Mail im Webmailer (Abb. 5) angezeigt. Aus diesem kann verschlüsselt geantwortet und die E-Mail, wenn gewollt, als Klartext ins System gespeichert werden. Der GINA-Webmailer ist bewusst möglichst einfach gehalten, um eine intuitive Anwendung zu ermöglichen.

© 2015 SEPPmail AG

Abb.5

**e) Funktionen im GINA-Webmailer:**

- **E-Mail lesen:** Schaltfläche zur Darstellung der geöffneten Originalmail (Abb. 5)
- **E-Mail schreiben:** Neue E-Mail verfassen die nur an einen Empfänger „hinter“ der SEPPmail-Appliance versendet werden kann.

Abb. 5a

Dabei können Anhänge mit beliebigem Format beigefügt werden. Eine Kopie der eigenen Antwort wird dem externen Beantworter GINA-verschlüsselt zurückgeliefert. (Abb. 5a)

- **Einstellungen:** Darin können Passwort, Mobilfunknummer und Sicherheitsfrage/-antwort verändert werden. (Abb. 5b)

© 2015 SEPPmail AG

Abb. 5b

- **Untermenü: Schlüssel/Zertifikate:**
  Der Externe Kommunikationspartner wird über ein Zusatzmenü in die Lage versetzt, eigenes Schlüsselmaterial dem SEPPmail Betreiber zur Verfügung zu stellen. Dabei kann durch die vorhergegangene 2-Faktor Authentifizierung (GINA-Mail + Initialpasswort per SMS) den Schlüsseln auch sofort getraut werden. Ein Validieren durch den Administrator ist an dieser Stelle nicht notwendig ! (Abb. 5c)

Abb. 5c

Andererseits bekommt ein externer Kommunikationspartner über die Schaltfläche "Suchen" optional auch das verfügbare Schlüsselmaterial (S/MIME; openPGP; Domänen Schlüssel) zur Verfügung gestellt (Abb. 5d):

© 2015 SEPPmail AG

Abb. 5d

- Nachricht-Beantworten: Über diese Funktionen kann eine sichere E-Mail-Antwort erstellt und versendet werden. Eine Kopie davon wird verschlüsselt an den externen Sender zurückgesendet (Abb. 5e)

Abb. 5e

- Speichern als…: E-Mail kann im Klartext gespeichert und in beliebigen Ordner verschoben werden Entweder als eml- (Standard E-Mail Format) oder im msg-Format (Outlook)
- Logout: Schaltfläche zum Verlassen des GINA Web-Mailers. Dabei wird der Cache des Browsers und der SEPPmail Appliance geräumt. Somit verbleibt einzig die verschlüsselte Original-GINA-Mail im System des Empfängers. Ausgenommen der Empfänger  hat sich eine Klartext-Kopie dazu abgelegt

**f) Zusatzmodul SSPM: Self Service Passwort Management**

© 2015 SEPPmail AG

Sollte der GINA-Mail Empfänger sein eigenes Passwort vergessen, besteht die Möglichkeit dieses zurückzusetzen (Abb. 6). In der Grundversion bewirkt dieses einen Call beim Administrator oder Helpdesk, der den Empfänger kontaktiert und nachdem dieser sich authentifiziert hat, wird ihm sein neues Passwort mitgeteilt.

Ist das SSPM Modul aktiv, dann hinterlegt der GINA-Mail Empfänger beim Registrieren eine Sicherheitsfrage und –antwort (Abb. 6a). Beim Passwort Reset wird Ihm dann, nachdem der GINA-Mail Empfänger seine selbst vergebene Sicherheitsfrage positiv beantwortet hat, das neue Passwort per SMS auf die hinterlegte Mobilnummer zugesendet. Durch diesen automatisierten Vorgang wird der Administrator oder Helpdesk entlastet und der GINA-Mail Empfänger zeitnah mit einem neuen Zugangspasswort versorgt. Bei der nun folgenden Anmeldung, wird der Empfänger zur Neuvergabe eines eigenen Passwortes aufgefordert.

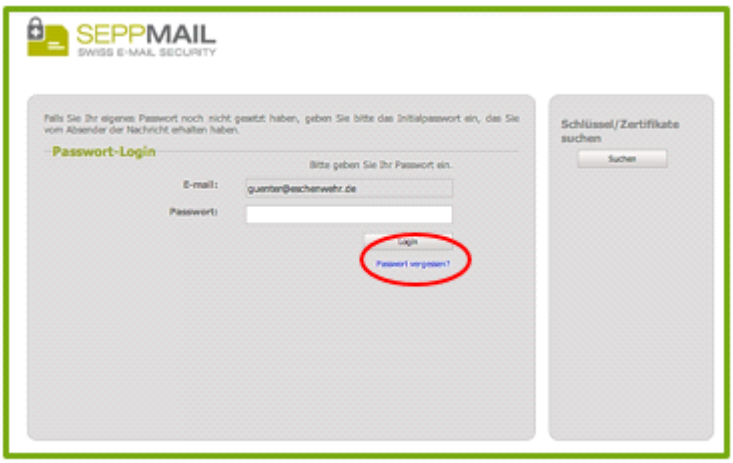



Abb. 6

Abb. 6a

**g) Der Entschlüsselungsvorgang**

Wie Eingangs schon erwähnt, benötigt der GINA-Mail Empfänger, ausser einem Client zum Empfangen von E-Mails und somit Internetzugang, sowie einen Browser keine weiteren

© 2015 SEPPmail AG

Komponenten. Beim Öffnen des HTML-Attachments und während der Eingabe des Zugangspasswortes, wird im Hintergrund über eine https-Strecke das Passwort geprüft und die E-Mail an die SEPPmail Appliance temporär zur Entschlüsselung eingeliefert und danach über den GINA-Webmailer im Klatext dargestellt.
(Abb. 7).

Sender
Empfänger
via https Strecke wird die verschlüsselte E-Mail beim Anmeldeprozess des Empfängers zum Entschlüsseln temporär an die SEPPmail Appliance gesendet
via https Strecke wird die entschlüsselte E-Mail zum Empfänger vollständig ausgeliefert.

Abb. 7

Die verschlüsselte E-Mail bleibt zu jeder Zeit im E-Mail System des Empfängers. Damit obliegt das Backup bzw. das Archivieren der E-Mail beim Empfänger. Ohne diese E-Mail hat er auch keine Möglichkeit diese über einen anderen Weg zu öffnen. Ein potentieller Angreifer benötigt daher beide Komponenten: E-Mail und Passwort. Eine „brute force“ Attacke ist nicht möglich, da die SEPPmail Appliance standardmässig nach 5 fehlerhaften Passworteingaben den Zugang sperrt.

### h) Zusammenfassung und Vorteile der patentierten GINA-Technologie

- Keine zusätzlichen Technologie-Layer bzw. Konvertieren in PDF, zip oder exe notwendig, da diese nur zusätzliche Komplexität und Fehlermöglichkeiten verursachen.
- Empfänger benötigt nur E-Mail Client, Browser und Internetzugang. Keinen PDF-Reader oder sonstige Verschlüsselungsclients am Empfängersystem.
- Wird vom Sender eine Lesebestätigung gewünscht, wird diese von der Appliance in dem Augenblick versendet, wenn die E-Mail zum Entschlüsseln eingeliefert wird. Diese kann vom Empfänger nicht unterbunden werden. Die Leseaktion wird immer im Log mit protokolliert.
- Das Zugriffspasswort kann jederzeit vom Empfänger geändert werden.
- Spontane sichere Kommunikation in beide Richtungen möglich
- Die E-Mails werden vollständig an Empfänger ausgeliefert, somit werden auf der SEPPmail nur Anmeldedaten und Keys gespeichert. (Für den Betreiber des sicheren E-Mail Gateways entfällt die Pflicht des Housekeepings (Archivierung) für E-Mails an Dritte).
- Alle Texte in der GINA Oberfläche können angepasst und das Aussehen per CSS-Stylesheet verändert werden. Im Auslieferungszustand sind die Sprachen Englisch, Deutsch, Französisch, Italienisch, Spanisch, Niederländisch und Polnisch integriert: Diese können beliebig erweitert (oder deaktiviert) werden
- Empfänger können sich auch am Portal vorgängig anmelden und so Ihre bevorzugte Verschlüsselungsform (Passwort oder Zertifikats-Key) wählen.

### i) Unterschiedliche Registrierungsprozesse für externe Kommunikationspartner

1. Spontaner Kommunikationsbeginn: Der Sender verfasst eine E-Mail, klassifiziert dieses als „Vertraulich“ und versendet diese. Hat er die Mobilnummer des Empfängers, könnte er diese im Betreff schon als Tag [zum Beispiel SMS:00491511234567] mitgeben. Die Appliance würde dann mit dem Versenden der GINA-Mail auch gleichzeitig das SMS auslösen.
   Ansonsten wird der Sender aufgefordert dem neuen Empfänger sein Initialpasswort auf parallelem Wege (SMS, Telefon, Fax) zu übermitteln.
2. Vorbereitete Kommunikation:
   a) Der Sender versendet eine Einladungsmail ohne Initialpasswort an den zukünftigen Kommunikationspartner. Diese sollte OHNE vertraulichen Inhalt sein. Der Empfänger öffnet

© 2015 SEPPmail AG

das HTML-Attachment und der unter Schritt 3 / Abb. 4 beschriebene Registrierungsprozess startet. Danach kann gesichert Kommuniziert werden. Der Externe hat sein eigenes Passwort festgelegt oder schon sein Schlüsselmaterial hochgeladen.

b) Der Externe meldet sich über die Webseite des SEPPmail Betreibers zur sicheren Kommunikation an. Ein Link bringt den externen Kommunikationspartner auf das Registrierungsportal der SEPPmail Appliance. Dort hinterlegt er sein Passwort (oder Schlüsselmaterial). Ein E-Mail Ping bestätigt seine Anmeldung:

SEPPMAIL
SWISS E-MAIL SECURITY
Die Aktivierungs-E-mail wurde an Ihre Adresse gesendet. Bitte folgen Sie den Anweisungen in der E-mail.

3. Die „harte“ Tour: Jede vertrauliche E-Mail wird per GINA und mit einem SMS-Passwort versendet.

© 2015 SEPPmail AG

#### 3.2.5.1 Mobile Computing Support

##### 3.2.5.1.1 Interne Nutzer von mobilen Endgeräten

Grundsätzlich gilt, dass SEPPmail dem internen Netzwerk vertraut. Somit sind alle E-Mails im Intranet und am E-Mail Server im Klartext verfügbar. Da die internen mobilen Endgeräte sich die E-Mails vom E-Mail Server ziehen und dort abliefern, ist von dieser Seite KEIN Problem zu erwarten.

Wie klassifiziert ein interner Nutzer auf seinem mobilen Endgerät (herstellerunabhängig) eine E-Mail als VERTRAULICH? Dies ist generell mit der Befehlsfunktion in der Betreffzeile möglich. Der Verfasser fügt ein festgelegtes Kommando - zum Beispiel [confidential] oder [sign] beziehungsweise ein vom Kunden individuell festgelegtes Befehlswort wie <c> - in die Betreffzeile ein. Die E-Mail wird am E-Mail Server angenommen, ausgeliefert und die danach folgende SEPPmail Gateway Appliance reagiert auf diesen Befehl und führt das entsprechende Kommando für Verschlüsseln oder Signieren aus.

Blackberry hat mit der Version 10.3.1 (erwartet für Februar/März 2015) eine E-Mail Klassifizierungsfunktion in seinem E-Mail-Client angekündigt. Genauere Details dazu sind SEPPmail noch nicht bekannt. (Stand Jan 2015).

Für die Standard E-Mail-Clients von iOS, Android und Windows Phone sind keine integralen Funktionen für das Klassifizieren von E-Mails bekannt. Sollten solche in zukünftigen Versionen implementiert werden, wird SEPPmail auch diese für das Ansteuern der eigenen Lösung nutzen. Werden Klassifizierungs-Plugins vom Kunden gewünscht, kann SEPPmail Machbarkeitserhebungen dazu anstellen, Nutzen und Aufwand abschätzen und eine Realisierung anstossen.

© 2015 SEPPmail AG

3.2.5.1.2 Externe Empfänger von verschlüsselten E-Mails auf mobilen Endgeräten

| Hersteller / Betriebssystem | Zertifikats-Unterstützung durch Vendor gegeben | Bemerkung |
|---|---|---|
| **Android** | ja | Eine Beispiel-Anleitung zum Import bzw. Installation auf iOS Geräten finden Sie hier: https://blog.globalsignblog.com/de-de/zertifikate-auf-android-ger%C3%A4ten-installieren |
| **Windows Phone** | ? | Keine Dokumentation im Netz vorhanden |
| **Blackberry 10 und höher** | ja / nein | Blackberry hat nach Auskunft des Supports bei signierten und verschlüsselten ein grundsätzliches Problem, welches so schnell auch nicht behoben werden kann. Das Fehlerverhalten von zum Beispiel signierten E-Mails auf BB Endgeräten ist unterschiedlich und nicht vorhersehbar. zum Beispiel bei einem Reply auf eine signierte E-Mail vom BB Client, verschwindet der Antworttext beim Empfänger. Das Problem kann nicht gefixt werden. |
| **iOS (Apple)** | ja | Eine Beispiel-Anleitung zum Import bzw. Installation auf iOS Geräten finden Sie hier: http://wiki.fernuni-hagen.de/helpdesk/index.php/Zertifikat_in_iOS_einbinden |

3.2.5.1.3 Kompatibiolitätsmatrix für Empfänger von GINA Web-Mails

| Hersteller / Betriebssystem | Unterstützung | Bemerkung |
|---|---|---|
| **Android** | nativ | mit vollwertigem Browser zum Beispiel Firefox oder Chrome |
| **Windows Phone** | nativ | |
| **Blackberry 10 und höher** | nativ | Für frühere Betriebssystem Versionen kann eine App zur Verfügung gestellt werden |
| **iOS (Apple)** | kostenlose SEPPmail App im iTunes Store verfügbar | Das iOS Sicherheitskonzept (Sandbox) erfordert eine einfach zu handhabende App zum Übergeben der verschlüsselten Daten aus dem E-Mail an den Browser. |

© 2015 SEPPmail AG

#### 3.2.5.2 Administration und Management

Eine komplette Managementoberfläche für die Administration und das Management der GINA-User ist integraler Bestandteil der Lösung. Auf diese Oberfläche ist ein rollenbasierter (Helpdesk) Zugriff möglich.

#### 3.2.5.3 MS-Outlook AddIn

Das Outlook AddIn ist absichtlich möglichst einfach gehalten. Im Standard werden lediglich im E-Mail x-header für das Steuern der Appliance gesetzt. Eine direkte Kommunikation zwischen AddIn und SEPPmail ist nicht notwendig.

Das von SEPPmail kostenfrei gelieferte Outlook AddIn unterstützt Microsoft Outlook 2007, 2010 und 2013 jeweils in der 32 und 64 Bit Version auf den Plattformen Microsoft Windows7 und 8.1 sowie Terminal Server jeweils in der 32 und 64 Bit Version

Das AddIn, kommt als MSI Installationspaket und kann somit mit den üblichen Software Verteil- und Installationsmechanismen customized problemlos in grossen Umgebungen ausgerollt werden. Weiterhin ist ein ADM-Template für die Konfiguration des AddIns per Group-Policies (GPO) vorhanden.

Eine detailierte Beschreibung der Konfigurationsmöglichkeiten ist im Kapitel Edit GINA Settings 165 zu finden.

### 3.2.6 Elektronische Signaturen

Die SEPPmail Appliance beherrscht neben der Verschlüsselung von E-Mails auch die RFC konforme Signatur. Eine Authentizität und Integrität der Daten bzw. der versendeten E-Mail ist durch das Anbringen einer elektronischer Signatur zu erreichen und möglich. Zusätzlich wird mit der Signatur der öffentliche Schlüssel des Absenders verbreitet, welcher für das Verschlüsseln von an den Absender gerichteten E-Mails benötigt wird.

Das für die Signatur erforderliche Benutzerzertifikat (siehe auch S/MIME (X.509) 20) kann bei Bedarf über eine MPKI (siehe Managed PKI 20) automatisch durch die Appliance bezogen oder manuell für den jeweiligen Benutzer importiert werden. Das bedeutet: Die dazu erforderlichen zentralen Funktionalitäten (eingebaute PKI, Konnektoren zu offiziellen CA's, automatische Zuweisungsfunktion der Zertifikate zu den Usern) sind in der SEPPmail standardmässig vorhanden und werden mit der Verschlüsselungslizenz dem Betreiber und Nutzer zur Verfügung gestellt.

© 2015 SEPPmail AG

## 3.3 Aufbau und Architektur

### 3.3.1 Appliance

SEPPmail stellt Appliances sowohl in Form von hochstabiler Industrie-Hardware, als auch für virtualisierte Umgebungen zur Verfügung. Die Hardware ist bei den Modellen 3500B und 5000B mit redundanten Komponenten (Netzwerkkarten, Power supply und HDD) ausgelegt.

#### 3.3.1.1 Hardwaremodelle

- Empfohlen bis 100 Postfächer beziehungsweise 50 Verschlüsselungs-User (Encrypt Lizenzen)

| SEPPmail 500B | Dimensions (HxWxD) | Desktop form factor (90 x 330 x 203 mm) |
|---|---|---|
| | Processor | Intel Atom D510 1.66Ghz Dual Core |
| | RAM | 1 GB SO-DIMM DDR2 PC-667 |
| | Storage | SATADOM 8 GB Flash Modul SLC |
| | Network Controller | 2x Intel 82574L Gigabit LAN |
| | Power Supply | 250W flexATX 80+ low noise PSU |

- Empfohlen bis 1000 Postfächer beziehungsweise 500 Verschlüsselungs-User (Encrypt Lizenzen)

| SEPPmail 1000B | Dimensions (HxWxD) | 19" 1U short rack form factor (43 x 426 x 356 mm) |
|---|---|---|
| | Processor | Intel Core i3-530 2.93 GHz Dual Core |
| | RAM | 2 GB DDR3 ECC PC-1333 |
| | Storage | 250 GB enterprise class SATA hard disk drive |
| | Network Controller | 2x Intel 82574L Gigabit LAN |
| | Power Supply | 260W PFC PSU |

- Empfohlen bis 7500 Postfächer beziehungsweise 5000 Verschlüsselungs-User (Encrypt Lizenzen)

| SEPPmail 3500B | Dimensions (HxWxD) | 19" 1U rack form factor (43 x 435 x 699 mm) |
|---|---|---|
| | Processor | Intel Xeon E5-2603 1.80 GHz 4 Core |
| | RAM | 4 GB DDR3 ECC PC-1333 |
| | Storage | 2x 146 GB SAS hard disk drive 15k (RAID 1) |
| | Network Controller | 4 Port Intel 82571EB Gigabit LAN |
| | Power Supply | 2x 460W Hot Plug PSU |

- Empfohlen bis 20000 Postfächer, die maximale Anzahl von Verschlüsselungs-Usern ist im Einzelfall zu prüfen

| SEPPmail 5000B | Dimensions (HxWxD) | 19" 2U rack form factor (87 x 446 x 699 mm) |
|---|---|---|
| | Processor | 2x Intel Xeon E5-2630 2.3 GHz 6 Core |
| | RAM | 12 GB DDR3 ECC PC-1333 |
| | Storage | 3x 300 GB SAS hard disk drive 15k (RAID 1 + HSP) |
| | Network Controller | 4 Port Intel 82571EB Gigabit LAN |
| | Power Supply | 2x 460W Hot Plug PSU |

Durch die Kaskadierbarkeit der Systeme über Cluster und eingebautem Load Balancing ist die Anzahl der User frei skalierbar.
Die angegebene Empfehlung basiert auf Durchschnittswerten für E-Mail-Durchsatz und -Grössen im Verhältnis zur Anzahl der Postfächer und kann daher im Einzelfall stark abweichen.

© 2015 SEPPmail AG

### 3.3.1.2 Virtualisierte Versionen

Verfügbar für die Virtualisierungsumgebungen:

- ESX (VMware)
- Hyper-V (Microsoft)
- HyperVisor (RedHat)

Systemanforderungen für Virtualisierung:

**SEPPmail VM500** (Empfohlen bis 100 Postfächer beziehungsweise 50 Verschlüsselungs-User (Encrypt Lizenzen)

- Anzahl vCPUs: 1
- Arbeitsspeicher: 1 GB
- Festplatte: 2 GB

**SEPPmail VM1000** (Empfohlen bis 1000 Postfächer beziehungsweise 500 Verschlüsselungs-User (Encrypt Lizenzen)

- Anzahl vCPUs: 2
- Arbeitsspeicher: 2 GB
- Festplatte: 5 GB

**SEPPmail VM3000** (Empfohlen bis 7500 Postfächer beziehungsweise 5000 Verschlüsselungs-User (Encrypt Lizenzen) **)**

- Anzahl vCPUs: 4
- Arbeitsspeicher: 4 GB
- Festplatte: 10 GB

**SEPPmail VM5000** (Empfohlen bis 20000 Postfächer, die maximale Anzahl von Verschlüsselungs-Usern ist im Einzelfall zu prüfen)

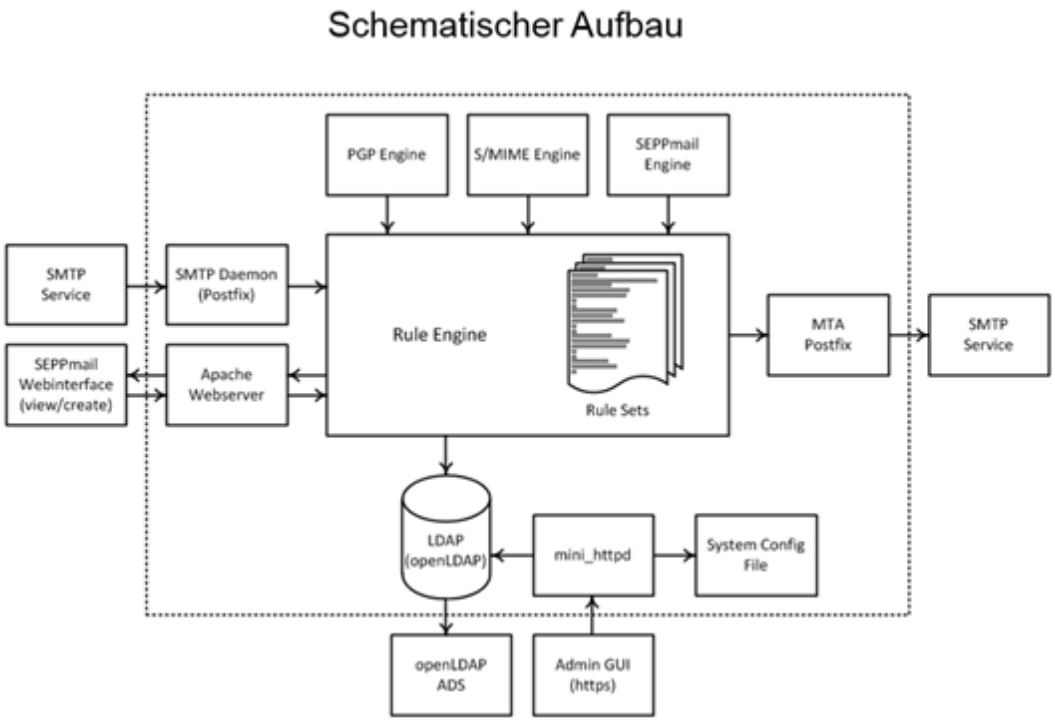
- Anzahl vCPUs: 12 empfohlen
- Arbeitsspeicher: 4 GB
- Festplatte: 20 GB

© 2015 SEPPmail AG

### 3.3.2 Software

Die Software basiert auf dem Betriebssystem openBSD, welches sich über die Jahre als extrem zuverlässig und widerstandsfähig gegen Angriffe erwiesen hat. Darüber hinaus wurde das Betriebssystem durch SEPPmail zusätzlich gehärtet. Die nicht benötigten Libraries wurden entfernt und nur die Module eingebaut, die für die Lösung erforderlich waren. Die Firmware hat in der komprimierten Version (Betriebssystem und Applikation) eine Grösse von ca. 60MB. Als MTA wird Postfix verwendet.

Das System ist so konzipiert, dass damit auch PCI – konforme Infrastrukturen aufgebaut werden können (Passwortregeln, SIEM, Samhain – Integration, verschlüsseltes Dateisystem etc.)




### 3.3.3 Zentrales Regelwerk (Rule Engine)

SEPPmail hat mit seiner Rule-Engine ein kleines Workflow-System eingebaut. Das Regelwerk kontrolliert den Fluss jeder einzelnen E-Mail durch die Applikation und definiert, welche E-Mail wie behandelt wird (signiert, verschlüsselt, entschlüsselt, zurückgewiesen,…).
Darüber hinaus können hier Prüfungen und Datenbankabfragen (LDAP-Lookups zum Beispiel an ein Microsoft Active Directory) durchgeführt und die retournierten Ergebnisse oder Parameter zur E-Mail Steuerung und/oder Verschlüsselungssteuerung herangezogen werden.

Dieses einfache und doch effektive Werkzeug ermöglicht die Definition eines Regelwerks, welches eine genaue Abbildung der gewünschten Security Policy eines Unternehmens darstellt. Die Rule-Engine ist als einfache if/else Skriptsprache aufgebaut. Eine umfassende Dokumentation des Aufbaus, der Befehle und der Parameter ist im Handbuch hinterlegt. Die Lösung wird mit einem Standardregelwerk ausgeliefert, welches in 90% der Fälle unverändert bei den Unternehmen zum Einsatz kommt und jederzeit den speziellen Bedürfnissen eines Unternehmens angepasst werden kann.

© 2015 SEPPmail AG

## 3.3.4 Architekturen

### 3.3.4.1 Im vollen Mailstrom

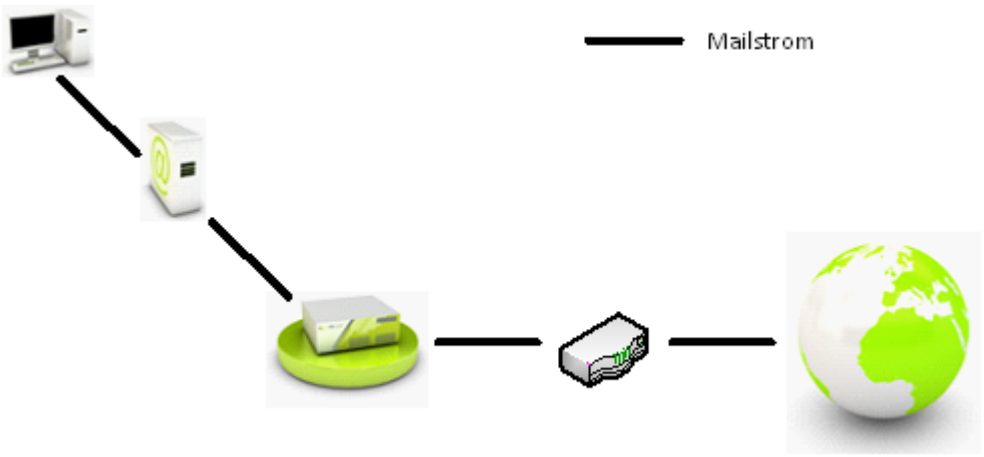
In den beiden folgenden Szenarien kann die Entscheidung, ob und wie E-Mails beim Versand verschlüsselt/signiert werden, zentral über das Ruleset der SEPPmail Appliance oder individuell am E-Mail Client via Schlüsselwörter, Outlook AddIn beziehungsweise IBM Notes Schablone oder Groupwise Vorlage getroffen werden.

Eingehende E-Mails werden gegebenenfalls entschlüsselt, beziehungsweise die Signatur geprüft und entsprechend für den internen E-Mail Empfänger gekennzeichnet (zum Beispiel [secure], [signed ok], [signed invalid])

Öffentliche Schlüssel von eingehenden, signierten E-Mails werden gesammelt, so dass diese zur Verschlüsselung an die absendenden Kommunikationspartner automatisch genutzt werden können. Eine Liste der zu gewährleistenden Kommunikationswege, über welche die SEPPmail Appliances kommunizieren ist sowohl im Quick-Install Guide (http://www.seppmail.ch/uploads/media/SEPPmail_Quick_Setup_Guide_02.pdf) als auch im Handbuch (http://www.seppmail.ch/uploads/media/SEPPmail_mit_Ruleset_v7.0.2_01.pdf) zu finden.

#### 3.3.4.1.1 Kleine Umgebungen

Für gewöhnlich wird die Appliance in kleineren Umgebungen als zusätzliche Stufe zwischen E-Mail Server und Internetzugang (Router) in den E-Mail Strom gesetzt. In dieser Konstellation wird für die Appliance optional ein „Protection Pack“ (Virus, Spam and Phishign Protection VSPP) für Spam Erkennung und Virenschutz angeboten.



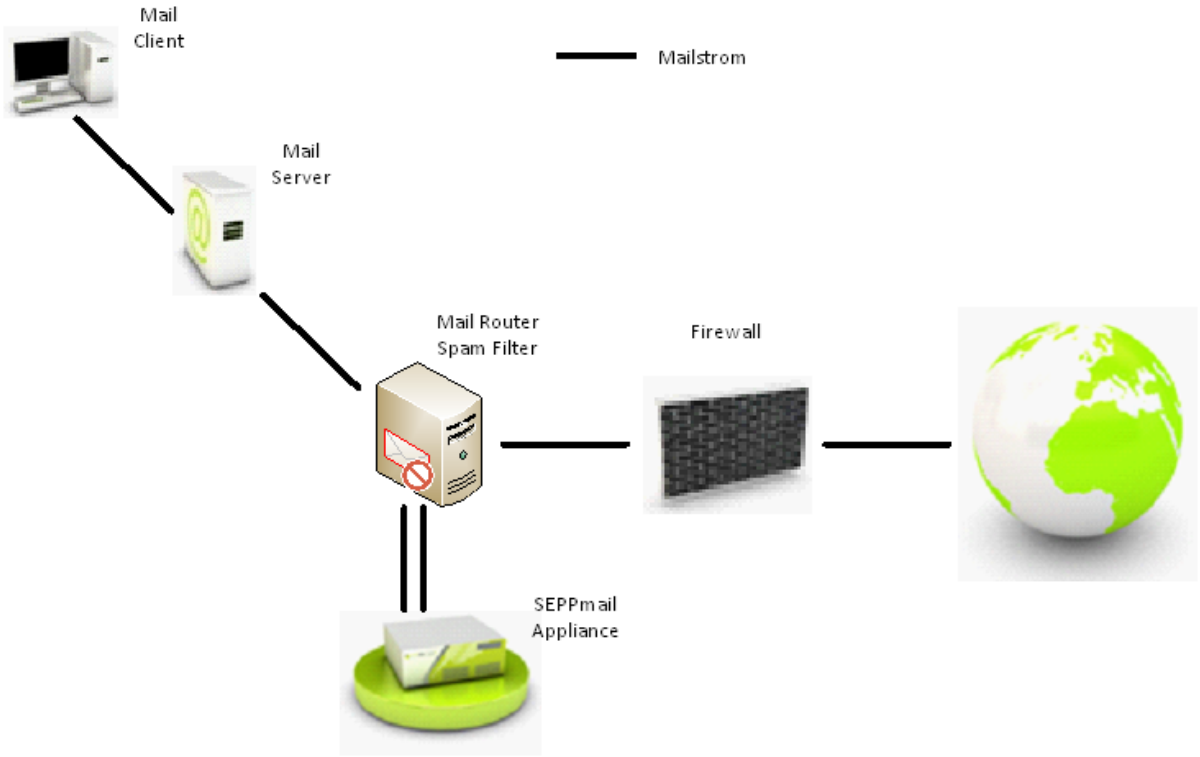

© 2015 SEPPmail AG

3.3.4.1.2 Grössere beziehungsweise komplexere Umgebungen

In grösseren Umgebungen trifft man häufig auf eine separate AntiSpam-/Antiviren- Lösung, welche im Normalfall auch E-Mail Routing Funktionen zur Verfügung stellt.

Dabei werden ausgehende E-Mails am Spam-Filter auf Viren geprüft, bevor sie gegebenenfalls an der Appliance verschlüsselt/signiert werden.

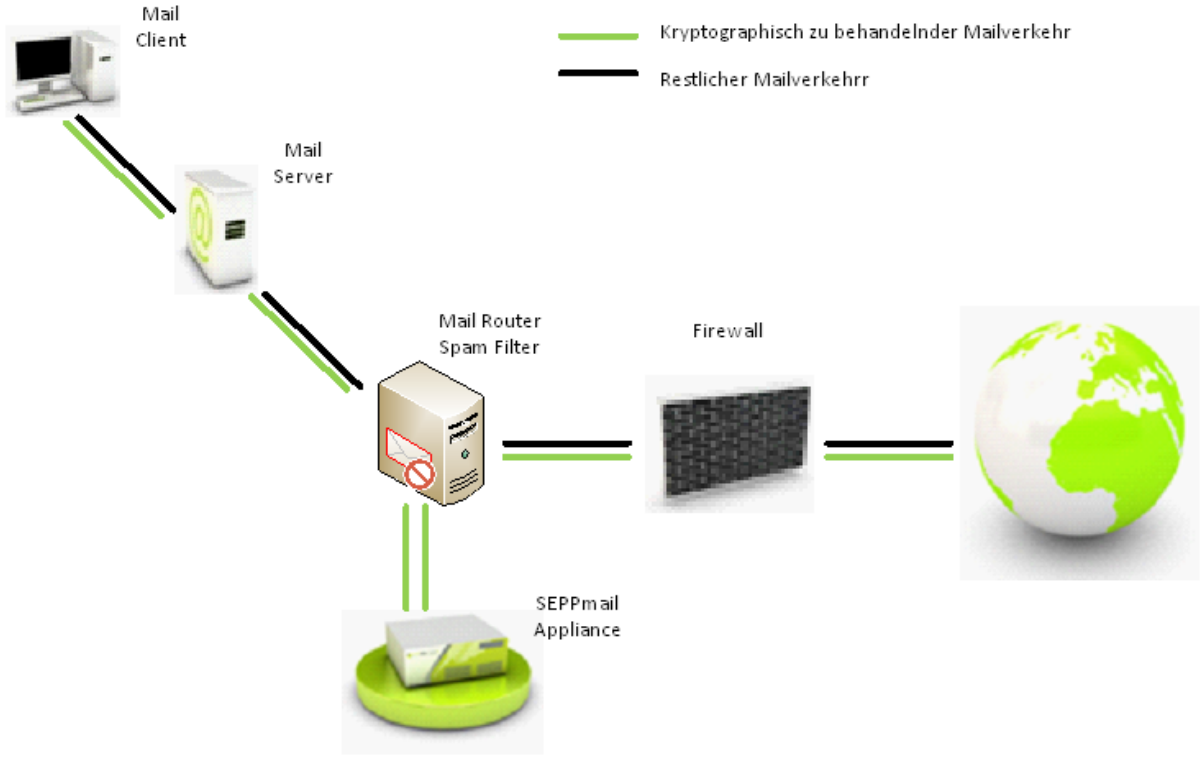
Eingehende verschlüsselte E-Mails werden zunächst zum Entschlüsseln an die SEPPmail Appliance geleitet und anschliessend zur Virenprüfung zurück an den Spam-Filter geliefert. Somit können auch verschlüsselte E-Mails an zentraler Stelle auf Viren geprüft werden.




© 2015 SEPPmail AG

### 3.3.4.2 Über spezielles Routing angesteuert

Im folgenden Szenario fällt die Möglichkeit des zentralen Entscheidens, ob und wie E-Mails beim Versand verschlüsselt/signiert werden, an der SEPPmail Appliance weg. Dieses Steuern wird von der vorgeschalteten AntiSpam- Komponente übernommen.
Hierfür muss diese ebenfalls die individuell am E-Mail Client via Schlüsselwörter, Outlook AddIn, IBM Notes Schablone oder Groupwise Vorlage getroffene Entscheidung interpretieren können.




### 3.3.4.3 Schnittstellen

Eine Liste der zu gewährleistenden  Kommunikationswege, über welche die SEPPmail Appliances kommunizieren ist sowohl im Quick-Install Guide (http://www.seppmail.ch/uploads/media/SEPPmail_Quick_Setup_Guide_02.pdf) als auch im Handbuch (http://www.seppmail.ch/uploads/media/SEPPmail_mit_Ruleset_v7.0.2_01.pdf) zu finden.

© 2015 SEPPmail AG

## 3.3.5 Hochverfügbarkeit, Loadbalancing

Die Cluster- und Loadbalancing-Funktionalität ist im Grundsystem der SEPPmail-Appliance integriert. Mit wenigen Schritten kann ein Cluster zwischen zwei und mehr Geräten aufgebaut werden, bei Bedarf auch über verschiedene Standorte hinweg. Dabei werden alle betriebsrelevanten Daten (Systemparameter, Nutzerdaten und Schlüsselmaterial) über alle Systeme synchronisiert. Die Systeme sind so ausgelegt, dass bei einem Totalausfall eines Standortes, der oder die verbleibenden Standorte den Betrieb reibungslos aufrechterhalten können. Sobald der Regelbetrieb wieder hergestellt ist, werden wieder alle Systeme automatisch abgeglichen.

### 3.3.5.1 Multi Master LDAP

Ein SEPPmail Cluster besteht aus zwei oder mehr SEPPmail-Appliances. Jeder Member des Clusters oder jede Instanz ist Teil des Multi-Master LDAP Verbundes. Im LDAP sind alle für den Betrieb einer Instanz notwendigen Daten abgelegt.

Der Einsatz von Multi-Master LDAP ermöglicht deshalb auf einfache und elegante Art allen Instanzen, mit minimaler Verzögerung, die gleiche Datenbasis zur Verfügung stellen.

Des Weiteren erlaubt das Verwenden von LDAP als Clusterprotokoll, einen Cluster auch über reine IP Netzwerke zwischen den Rechenzentren zu betreiben. Layer 2 Netzwerke oder Spezialprotokolle zwischen den Netzwerken sind in aller Regel nicht notwendig.

### 3.3.5.2 Queue-Less-Betrieb

SEPPmail hat eine einzigartige Funktionsweise, bei der E-Mails nie in einer Queue und nie auf der Appliance zwischengespeichert werden. Eine E-Mail wird erst dann als empfangen quittiert, wenn sie an den nächsten Server weitergereicht wurde.

Dadurch muss auf den Appliances kein Platz für grosse Queues vorgehalten und überwacht werden. Ein Backup der Queue ist ebenfalls nicht notwendig, da keine Nutz-Mails in Queues gelagert werden.

Dieses Verfahren führt zu einer erheblichen Erleichterung bei der Fehlersuche im E-Mail System. Hauptsächlich aber kann damit eine Appliance bei Hardware Ausfall garantiert ohne Datenverlust ausgewechselt werden.

### 3.3.5.3 Cluster: Multimaster LDAP & Queue-Less Betrieb

Durch das Verwenden des Queue-Less Modus und den Einsatz GINA-Technologie, werden keinerlei E-Mails in den Appliances gelagert und müssen deshalb auch nicht zwischen den Geräten zur Ausfallsicherheit synchronisiert werden. Die Datenmenge, die zwischen den Instanzen ausgetauscht werden muss, ist deshalb sehr klein: Es müssen nur Konfiguration und Schlüssel Material synchronisiert werden.

### 3.3.5.4 Fail-Over und Loadbalancing

Mit wenigen Schritten kann ein Cluster zwischen zwei und mehr Geräten aufgebaut werden, dies auch verteilt über verschiedene Standorte. Der Multimastercluster benötigt dabei einzig eine TCP–Verbindung zwischen den Geräten.

Fail-Over kann in mehreren Stufen realisiert werden:

- Durch das Verwenden von MX – Records für das Ansprechen der Systeme
- Durch das Definieren von (lokalen oder allgemein verfügbaren) DNS – Einträgen mit MX –

© 2015 SEPPmail AG

Records für den nächsten Hop
- Durch Definition von virtuellen IPs, wobei die IPs eines ausfallenden Systems automatisch von einem der verbleibenden Geräte übernommen wird

Load-Balancing kann in mehreren Stufen realisiert werden:

- Durch Aufteilen des E-Mail Stroms auf verschiedene virtuelle IPs (zum Beispiel ein – und ausgehender E-Mail Verkehr getrennt)
- Durch Definition von MX–Records mit gleicher Priorität auf virtuelle IP–Adressen oder DNS Round Robin
- Zusätzlich hat jede SEPPmail einen integrierten Loadbalancer: Wenn eine Maschine überlastet ist, werden Aufgaben automatisch an vordefinierte andere Maschinen weitergegeben. Dies funktioniert auch über verteilte Standorte

Für den Zugriff auf das Webportal (GINA) wird das Verwenden von virtuellen IPs und eventuell eine Web Application Firewall (WAF) empfohlen.
Da praktisch alle Installationen von SEPPmail mit einem Cluster arbeiten (insbesondere bei Verwenden von Hardware–Appliances) ist die eingesetzte Technik praxiserprobt und extrem zuverlässig.

© 2015 SEPPmail AG

## 3.3.6 System Management

### 3.3.6.1 Administration

Der administrative Zugriff erfolgt in der Regel über eine SSL gesicherte Verbindung auf einen separaten Web Server.

### 3.3.6.2 Rollenrechte

Die SEPPmail Appliance hat ein integriertes Rollen-Rechtesystem. Dieses ist in der folgenden Tabelle abgebildet:

| Rolle | Zugriff |
|---|---|
| admin | Vollzugriff |
| administrationadmin | Systemrelevante Konfigurationseinstellungen (Lizenz, Update, Backup, Importfunktionen, Boot) |
| backup | Das Backup der Appliance wird täglich verschlüsselt an die E-Mail-Adressen aller Backup Benutzer gesendet |
| caadmin | Interne Certificate Authority (CA) und Managed Public Key Infrastructure (MPKI)-Einstellungen |
| clusteradmin | Cluster Einstellungen |
| domainkeysadmin | Domänen Schlüssel Verwaltung |
| groupsadmin | Gruppenverwaltung (diese beinhaltet sowohl die hier beschriebenen Rollen, wie auf optional selbst erstellte Gruppen zur Verwendung im RuleSet) |
| homeadmin | Übersicht des Systemstatus |
| logsadmin | Logs |
| mailprocessingadmin | Rule Engine |
| mailsystemadmin | Anbindungseinstellungen und einfache AntiSpam Einstellungen |
| multiplecustomersadmin | Mandanteneinstellungen in multitenant Systemen |
| openpgpkeysadmin | openPGP Schlüsselverwaltung |
| readonlyadmin | lesender Zugriff auf alle Menüs |
| ssladmin | SSL Einstellungen |
| statisticsadmin | Statistik Graphiken |
| systemadmin | Systemeinstellungen (Netzwerkinterfaces) |
| usersadmin | Interne Benutzerverwaltung |
| webmailaccountsadmin | GINA Benutzerverwaltung |
| webmaillogsadmin | GINA Webmail Logs |
| x509certificatesadmin | X.509 Zertifikatsverwaltung |
| x509rootcertificatesadmin | X.509 Root Zertifikatsverwaltung |

© 2015 SEPPmail AG

#### 3.3.6.3 Backup / Restore

Das System wird täglich automatisch gesichert. Inhalt der Sicherung ist ausschliesslich Konfiguration und Schlüsselmaterial, weshalb die Grösse der Sicherung selbst nach jahrelangem Betrieb der Appliance minimal bleibt. Die Sicherungsdatei wird automatisch verschlüsselt an den oder die BackupOperator gesendet. Da auf den Appliances dank der GINA-Technologie nie Nutzdaten gespeichert werden müssen, kann im Disasterfall trotz der geringen Grösse des Backups die volle Funktionalität des Systems innerhalb kürzester Zeit wiederhergestellt werden.

Der Restore einer einzelnen Maschine erfolgt durch das alleinige Einspielen der Backupdatei nach dem Neustart.

Der Restore einer Clustermaschine erfolgt automatisch per Replikation nach Aufnahme der neuen Maschine in den bestehenden Cluster.

#### 3.3.6.4 Systemupdate

Das System sucht regelmässig nach anstehenden Versionsupdates und Patches und zeigt anstehende Updates dem Administrator an. Dieser entscheidet, ob er das Update „prefetchen“ oder sofort durchführen möchte. Dabei wird immer das gesamte Core-System (Firmware) ausgetauscht, d. h. keine Einzelkomponenten. Erhalten bleiben hingegen alle Systemeinstellungen, kundenspezifische Anpassungen und das Schlüsselmaterial.

Bei einem Clusterbetrieb, können im Wartungsfall die Komponenten einzeln und im laufenden Betrieb einem Systemupdate unterworfen werden Ein Aufbrechen des Clusters ist möglich, aber nicht notwendig. Da die Software als echte Firmware ausgeliefert wird, sind Systemupdates sehr gut planbar, da nicht einzelne Komponenten (zum Beispiel Datenbanken und Module) auf voneinander abhängige Release-Stände gezogen werden müssen. Auch ist die Lösung dadurch im Voraus zu testen.

#### 3.3.6.5 SysLog

Die SEPPmail-Appliance bietet die Möglichkeit ihre gesamten Logs an SysLog Server zur zentralen Überwachung/Archivierung zu liefern. Die RFC 3164 Konformität ist gegeben.

Neben dem Mail Log können bei Bedarf alle Admininistrationsoberflächen- wie auch GINA- Ereignisse in einem PCI konformen Format eingerichtet werden (CEF – Format zum Beispiel für ArcSight).

#### 3.3.6.6 Report

Ein Statusreport wird einmal täglich von der Appliance per E-Mail sowohl an den Administrator wie auch dem Statistik-Verantwortlichen versendet. Dabei werden Notifications und Warnings angezeigt, wieviele Root Certificate zur Prüfung anstehen und je eine graphische Statistik zu Durchsatz (Reseived-Sent-Encrypted-Decrypted), Technologie (Webmail-S/MIME-openPGP-Domain), optional Spam (incoming-Spam-Blacklisted-Greylisted), Prozessor- und Speicherauslastung ausgeworfen. Darüber hinaus stellt das System auch noch Reports im csv-Format zur Anzahl der versendeten oder empfangenen E-Mails und den verwendeten Technologien pro Benutzer und Domäne zur Verfügung.

© 2015 SEPPmail AG

# SEPPmail Daily Report for Device ID 0050-56a6-4706

## Notifications and Warnings

**NOTE:** There is a new version available: Installed version is 7.1.1-dev Build 4944, latest version is 7.1.1-dev Build 4948

## Root Certificates

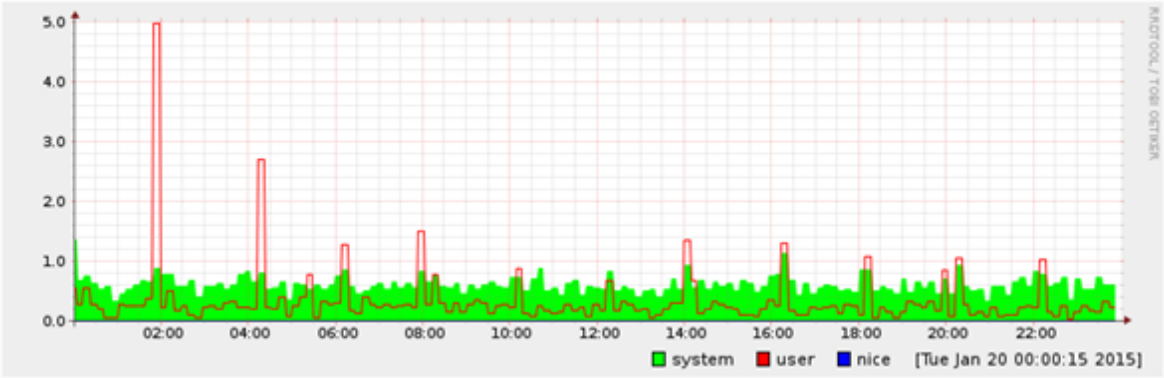
**NOTE:** There are 29 Root Certificates with undefined state.

To get rid of this message, log in to your appliance and click on "X.509 Root Certificates"
Click on each entry with a "?" and decide if you want to trust the certificate or not.
A good way to decide if you want to trust a certificate is to download it and to check if your PC trusts the certificate.

## Statistics

### Throughput Visualisation

### CPU Usage




© 2015 SEPPmail AG

### 3.3.7 Mandantenfähigkeit - Public-/Private Cloud Implementierung

SEPPmail-Appliances sind grundsätzlich mandantenfähig.
Somit wird Unternehmensrechenzentren und Managed Service Providern ermöglicht den Service „Sichere E-Mail“ auch für eigenständige Unternehmenseinheiten und/oder unterschiedliche kleinere oder grössere Kunden (Mandanten) anzubieten. Dabei unterliegt der Betrieb der Appliance dem Provider.

Durch eine ebenfalls nach Mandanten getrennte Konfigurationsoberfläche, kann über optional jeweils einzurichtende Mandanten-Admins, der jeweilige Mandant spezifische Aufgaben selbst übernehmen, wie zum Beispiel

- Vornehmen von GINA-Einstellungen und Layouts
- Prüfen von Log-Dateien
- Verwalten von SEPPmail-Benutzern (für die Signierung/Verschlüsselung)
- Verwalten von GINA--Benutzern
- Verwalten von LFM-Benutzern (optional)

Die Art und Weise der E-Mail Verarbeitung wird jedoch grundsätzlich zentral verwaltet und ist somit für jeden Mandanten identisch.

Das bedeutet der MSP macht seinen Kunden Vorgaben bezüglich der E-Mail Verarbeitung !
Diese ist im Ruleset definiert und enthält zum Beispiel:

- Merkmale für das Steuern der Appliance
  - Tags (zum Beispiel [confidential], [sign] usw.)
  - E-Mail Header (Sensitivity-Parameter welcher zum Beispiel aus dem Outlook Vertraulichkeitsflag resultiert)
  - X-Header (zum Beispiel aus dem kostenfreien Seppmail Outlook AddIn)

- Tags für das Rückmelden durchgeführter Aktionen
  - Tags (zum Beispiel [secure], [signed ok] usw.)
  - Header (Setzen des Sensitivity-Parameter (Vertraulichkeits-Flag))

- Automatisches Erzeugen von SEPPmail-Benutzern
- MPKI von welcher CA Zertifikate automatisiert bezogen werden.

Ist jedoch das zur Verfügungstellen von unterschiedlichen Verfahrensweisen der E-Mail Verarbeitung (Ruleset Einstellungen, unterschiedliche MPKI) pro Mandant unumgänglich, so kann dies durch 2 Arten gelöst werden:

- Installieren von mehreren Instanzen mit unterschiedlichen Rulesets.
- Das Standard-Ruleset so anzupassen, dass die unterschiedlichen Regelbedürfnisse pro Mandant in diesem abgebildet werden (siehe auch **Zentrales Regelwerk (Rule Engine)** 38)

© 2015 SEPPmail AG

## 3.4 Sicherheit

**Sicherheitkonzept des Betriebssystems openBSD**

SEPPmail hat das, an sich als gut gesichert bekanntes Betriebssystem, zusätzlich im „Bottom-up“ Verfahren gehärtet. Dabei wurden alle nicht notwendigen Libaries entfernt und nur jene unbedingt notwendigen Funktionen behalten.
Bei der Lösung handelt es sich um eine “echte” Firmware: Bei einem Update wird das Gesamtsystem aktualisiert. Damit ist dieses auch test- und reproduzierbar.

**Sicherheitskonzept Core Application**

Bei der Appliance handelt sich um eine gekapselte Applikation. Alle Schnittstellen gegen aussen sind möglichst einfach gehalten und nur die absolut notwendigen wurden implementiert. Die Firmware ist gepackt mit allen zugehörigen Applikationen rund 60 MB gross.

**Sicherheitskonzept GINA**

Das Webinterface wurde absichtlich sehr einfach gehalten und nur mit den absolut notwendigen, aber ausreichenden Funktionen versehen. Zur Eingabe werden nur genau vordefinierte Datenfelder akzeptiert. Jedes Datenfeld wird beim Einliefern auf Gültigkeit geprüft. Der gehärtete Webserver läuft als unprivilegierter User.

**Schutz der Daten**

- CA-Schlüssel, Private Schlüssel, Session Schlüssel, GINA Benutzer Schlüssel
  - Die Hauptmaschinen sind so gekapselt in der DMZ platziert, dass keinerlei direkter Zugriff von aussen möglich ist.
  - Sollte der Wunsch/Forderung bestehen, dass die PKI-Daten ausschliesslich im Intranet abgelegt werden, kann die Lösung aufgetrennt werden. Dabei werden für den Web-Zugriff (GINA) eigene Maschinen (Satelliten) ohne eigene Datenhaltung in der Internet DMZ verwendet.
  - In der Regel macht das Sicherheitskonzept der Appliance in Kombination mit den vorhandenen Überwachungsmöglichkeiten (SamHain, Audit Log, SNMP etc.) ein HSM unnötig. Sollte dennoch ein zusätzliches Sicherung von privaten Schlüsseln gewünscht sein, ist das Anbinden einer HSM (zum Beispiel durch Thales oder Safenet) möglich.

- Pin/Passwörter
  - Passwörter dienen dem Zugriff eines externen Empfängers auf seine GINA-E-Mail bzw. nachgelagert dem AES256 Schlüssel auf der Appliance zum Entschlüsseln seiner E-Mail. Letzterer verlässt die gut geschützte SEPPmail-Appliance niemals.

**Zertifizierungen**

Die Appliance kann auch für den Betrieb in PCI – konformen Umgebungen konfiguriert werden. Zum Beispiel hat die Lufthansa Systems ein PCI – konformes Gesamtsystem mit einer SEPPmail-Appliance als Kernsystem aufgebaut. Im Oktober 2014 wurde das System mit positivem Abschluss geprüft.

Aus unserer Sicht ist es derzeit aus unterschiedlichen Gründen fraglich, ob und welche „standardisierten“ Zertifizierungen sinnvoll sind. Der Markt der „Sicherheitszertifizier“ wächst schnell und ist unübersichtlich. Einige ausländische Unternehmen verlangen zudem Einblicke in den Sourcecode. Dies können wir aus sicherheitsrelevanten Gründen nicht zulassen.

Die von der Lufthansa Systems durchgeführte Prüfung auf PCI-Compliancy ist unseres Erachtens

© 2015 SEPPmail AG

deutlich strenger und daher höher zu bewerten, da diese neben einem normalen PenTest sehr harte Vorgaben bezüglich Zugangsrechte und Protokoll der Administrationstätigkeit verlangt und prüft.

**Aktuelle Sicherheitslücken oder Exploits**

SEPPmail reagiert – falls betroffen - auf bekannt werdende Sicherheitslücken oder Exploits innerhalb kürzester Zeit mit einem Sicherheitsupdate, welcher allen Kunden über den normalen Update-Mechanismus zur Verfügung gestellt wird.
Die kürzlich bekannt gewordenen Sicherheitslücken wie „Heartbleed“ oder „Poodle“ betrafen die Lösung nicht.

© 2015 SEPPmail AG

## 3.5 Zusätzliche Features

Die SEPPmail-Appliance bietet zusätzlche Features, welche auf Wunsch beziehungsweise bei Bedarf lizensiert und verwendet werden können.

### 3.5.1 Large File Management (LFM)

**Einführung**

Das Problem der übergrossen E-Mail Anhänge ist den Meisten bekannt. Sobald eine bestimmte E-Mail Grösse überschritten wird, wird die E-Mail entweder schon vom eigenen oder aber vom E-Mail Server des Empfängers abgewiesen. Danach beginnt die Suche nach einem geeigneten Übermittlungsverfahren. Zur Verfügung stehen dann: fFTP-Server, diverse Web-Angebote wie Zum Beispiel dropbox oder der Postweg für die selbst gebrannte DVD.

SEPPmail nutzt die Basisfunktionalität der Appliance und den Einladungsprozess der GINA-Technologie, um dieses Problem elegant und für den User transparent zu lösen.
Dabei gibt zwei Möglichkeiten übergrosse E-Mails bei der SEPPmail-Appliance einzuliefern:

- Standard E-Mail Client
- GINA Web-Mail Client

Auf der Appliance selbst sind nur vier Parameter einzustellen:

- Grösse der E-Mail (in kB) ab welcher die LFM Funktionalität aktiv wird.
- Maximalgrösse einer LFM Mail
- Verweildauer (in Tagen) nach welcher die E-Mail von der SEPPmail-Appliance gelöscht wird.
- Anzahl der LFM-Mails pro Nutzer. Damit werden die Appliance Ressourcen geschont und Massenversendung von übergrossen E-Mails unterbunden.

**Versenden von übergrossen Files via Standard E-Mail Client**

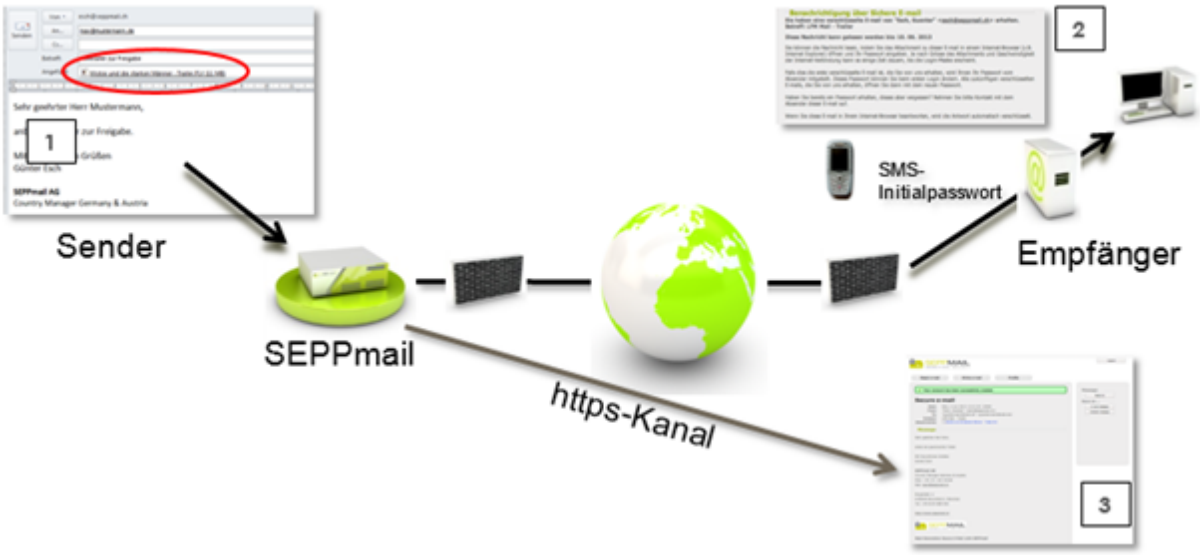
Wenn vom Betreiber des E-Mail Systems für den Sender keine Limitation der E-Mail Grössen vorgegeben ist, oder es keine sensiblen Daten sind, die PCI-compliant übermittelt werden müssen, steht der Nutzung des Standard E-Mail Clients zum Versenden von übergrossen Daten nichts im Weg.

Der Anwender verfasst in seinem gewohnten E-Mail-Client eine E-Mail und fügt seine zu übermittelnden Daten und Files als Anhang bei (1). Danach versendet er diese, ohne weitere Markierung oder Aktion. Sobald die gesamte E-Mail das auf der SEPPmail eingestellte Volumen übersteigt, wird diese verschlüsselt und auf der Appliance in einem gesonderten Datenbereich abgelegt. Gleichzeitig wird eine Einladung (2) zum Download der übergrossen E-Mail mittels GINA-Technologie versendet. Siehe Kapitel GINA Webmail 23.
Der Unterschied zu einer verschlüsselten E-Mail liegt darin, dass die Einladungsmail mit einem Ablaufdatum versehen ist und die Datei als solches nur wenige kByte gross ist.

Sobald der Empfänger den GINA Anmeldeprozess durchlaufen hat, wird die E-Mail samt Anhang auf der SEPPmail-Appliance entschlüsselt und steht zum Download über die etablierte https-Strecke und zum lokalen Speichern bereit (3).

Die E-Mail wird nach Erreichen der Verweildauer von der SEPPmail-Appliance gelöscht, auch wenn der Download noch nicht stattgefunden hat.

© 2015 SEPPmail AG

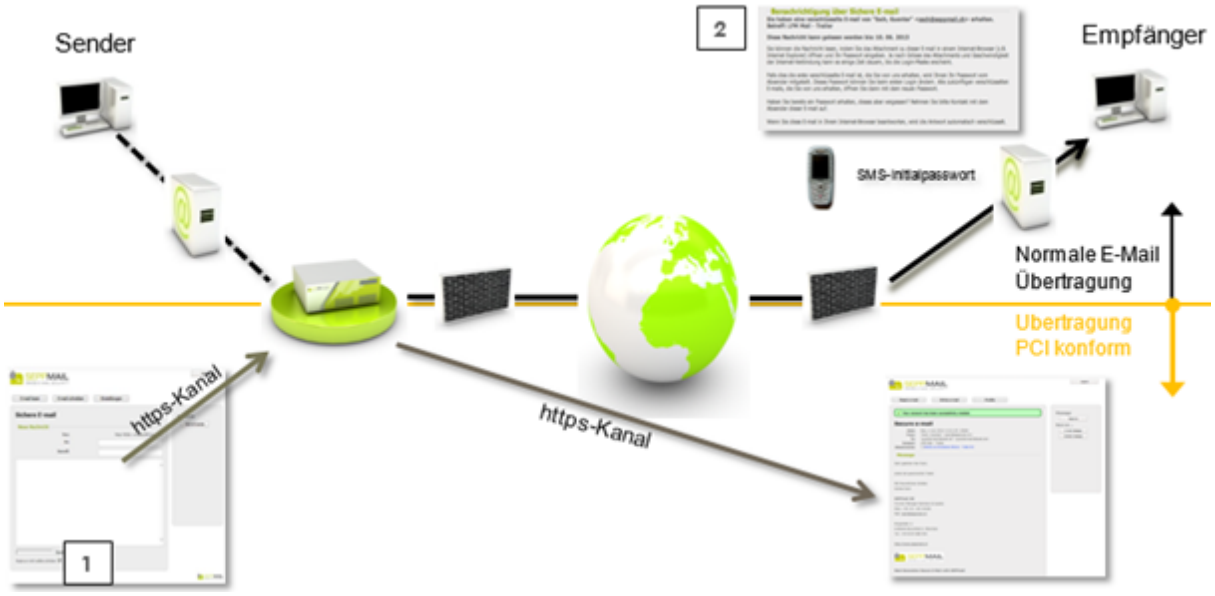



**Versenden von Daten via internem GINA Web-Mail Portal**

Da Storage teuer ist, tendieren manche IT-Abteilungen dazu, auch den ausgehenden E-Mail Verkehr von der Grösse her zu limitieren. Aber auch sensible Daten, wie zum Beispiel Kreditkarteninformationen, müssen über einen PCI konformen Übermittlungsweg übertragen werden. Fast alle E-Mail Systeme sind dafür nicht ausgelegt. SEPPmail kann in einem System beide Szenarien abbilden.

Der Anwender öffnet dafür den internen <%OEM-WEBMAIL-GINA> Webmail Client über seinen Browser und verfasst darin seine Nachricht und fügt die zu übermittelnden sensiblen Daten bei (1). Danach versendet er die Nachricht, wobei diese über den gesicherten https-Kanal auf die SEPPmail eingeliefert wird. Der restliche Vorgang ist mit dem unter Kapitel „Versenden von übergrossen Files via Standard E-Mail Client“ identisch. Die E-Mail samt Anhang wird verschlüsselt in einem gesonderten Datenbereich der Appliance abgelegt und es ergeht eine Aufforderung zur Abholung (2) an den oder die Empfänger. Dieser meldet sich mit seinem Initialpasswort oder eigenem Passwort an und lädt die Dateien auf sein System. (3)

© 2015 SEPPmail AG




Optional kann bei Bedarf für LFM die Passwortabfrage individuell abgeschaltet werden

**LFM – Antwort**

Dem Empfänger steht für eine Rückantwort der gleiche Kanal zur Verfügung. Er kann somit eine gesicherte E-Mail bzw. auch grosse vertrauliche Daten via dem GINA-Webmail Client übermitteln. Dazu bedient er sich der Antwortfunktion innerhalb des GINA-Clients.

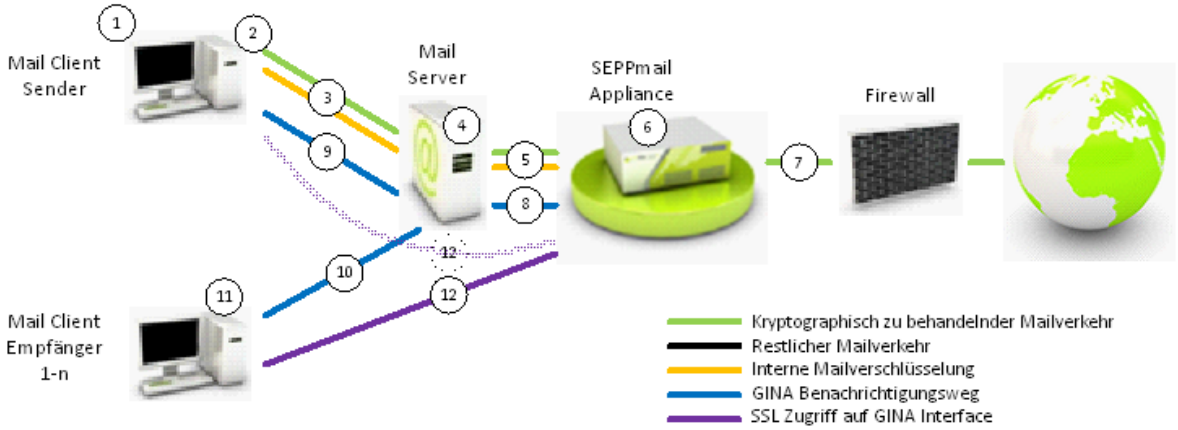
Der Prozess ist exakt invers zu der Versendung.

© 2015 SEPPmail AG

### 3.5.2 Internal Mail Encryption (IME)

Die SEPPmail-Appliance bietet wir optional die Möglichkeit der internen E-Mail Verschlüsselung. Um jedem Kundenbedarf gerecht zu werden stehen hierfür drei Konzepte zur Verfügung.

**Das erste Konzept**
basiert auf der GINA-Technologie in Verbindung mit dem Outlook AddIn. Die folgende Graphik zeigt den funktionalen Ablauf:




a) Am E-Mail Client (1) wird eine neue E-Mail – an einen oder mehrere interne und gegebenenfalls externe Empfänger - erzeugt.

b) Diese wird über das Outlook AddIn (2) als „zu verschlüsselnd“ und „intern zu verschlüsselnd“ markiert und modifiziert.

c) Die modifizierte E-Mail (3) wird an den E-Mail Server (4) geleitet.

d) Durch die vorgenommene Modifikation behandelt der E-Mail Server (4) die E-Mail an die internen Empfänger wie eine Internet E-Mail (5) und leitet diese somit an die SEPPmail-Appliance (6) weiter.

e) Die SEPPmail-Appliance (6) leitet die E-Mails an die externen Empfänger (7) „best effort“ verschlüsselt in das Internet.

f) Für die internen Empfänger generiert die SEPPmail-Appliance – sofern nicht bereits vorhanden - neue, interne GINA-Benutzer und versendet an diese sowie an den Absender die bekannte GINA-Mail (8) über den internen E-Mail Server (4).
Wurde vom Absender die interne E-Mail Verschlüsselung gewählt, jedoch nur externe Empfänger adressiert, so erhält an dieser Stelle natürlich nur er seine ausgehende E-Mail als GINA-Mail.

g) Der interne E-Mail Server stellt die GINA-Mail(s) (9)/(10) für den Absender (1) und den/die Empfänger (11) bereit.

h) Das AddIn (2) entfernt die noch unverschlüsselte E-Mail aus dem „Gesendet“ Ordner des Absenders (1). Dieser erhält an deren statt die GINA verschlüsselte E-Mail (9).

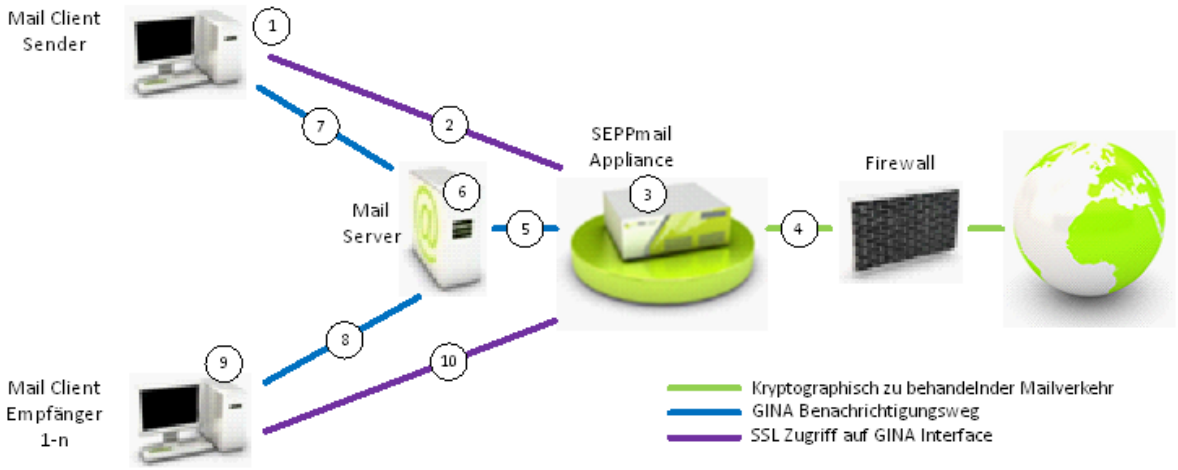
i) Der Absender (1) sowie die Empfänger (11) verbinden sich durch Öffnen des in der GINA-Mail befindlichen html-Anhangs mit dem GINA-Portal (12) der SEPPmail-Appliance (6), wo die E-Mail nach Anmelden mit den persönlichen Zugangsdaten gelesen werden kann.

Der Vorteil dieser Lösung liegt zum Einen in der Outlook-Integration, zum Anderen erleichtert Sie das Realisieren von Vertreterregelungen, da die intern verschlüsselten E-Mails auch verschlüsselt im Outlook abgelegt bleiben und somit nur vom originären Empfänger mit dessen Passwort entschlüsselt

© 2015 SEPPmail AG

und somit gelesen werden können.

**Das zweite Konzept**
basiert allein auf unserer GINA-Technologie, wobei sich der Versender bereits für den Versand der E-Mail am GINA-Portal anmeldet.




a) Am E-Mail Client (1) wird eine SSL Verbindung (2) zum GINA-Webinterface der SEPPmail-Appliance (3) aufgebaut.

b) Nach Anmelden am GINA-Webinterface wird im Webmailer direkt eine E-Mail an interne (und gegebenenfalls externe) Benutzer adressiert und versendet.

c) Die SEPPmail leitet die so erzeugten, bekannten GINA-Mails (5) an den internen E-Mail Server (6) (sowie für eventuell adressierte externe Benutzer (4) in das Internet).

d) Der Interne E-Mail Server (6) leitet die GINA-Mails an den/die Empfänger (8) sowie den Absender (7).

e) Die Empfänger (9) sowie der Absender (1) können die E-Mail im E-Mail Client öffnen und gelangen durch Öffnen des verschlüsselten HTML-Anhanges über die SSL-verschlüsselte Strecke [(10) beziehungsweise (2)] zum bekannten GINA-Webmailer (3) mit dessen Hilfe die ursprüngliche E-Mail aus dem HTML-Anhang entschlüsselt und gelesen werden kann.

Vorteil dieser Lösung ist die absolute Unabhängigkeit von den dazwischen eingesetzten Komponenten wie E-Mail Client oder E-Mail Server.

**Das dritte Konzept**
macht es erforderlich Schlüssel an die Clients zu verteilen. Diese können

a) von einer Self Signed CA stammen.
Dabei müssen den Usern ihre privaten Schlüssel zugänglich gemacht werden (zum Beispiel per GPOs). Auf der Appliance muss das Schlüsselmaterial ebenfalls vorliegen. Die öffentlichen Schlüssel werden intern über die Key Server Funktion der SEPPmail-Appliance für die interne Verschlüsselung bereitgestellt.
Wird eine E-Mail sowohl an interne als auch externe Empfänger gesendet, wird diese an der SEPPmail für den externen Versand „best effort“ umverschlüsselt/signiert.
Ein AddIn ist hier nicht notwendig, es reicht das S/MIME – Zertifikat auf allen Clients und die Angabe der SEPPmail als LDAP – Adressbuch. Es können somit die „eingebauten“ Verschlüsselungsfunktionen des E-Mail Clients benutzt werden.

© 2015 SEPPmail AG

b) von der SEPPmail-Appliance über den CA Connector bezogen werden und im Anschluss an den User verteilt werden.
Damit wird auch intern das Schlüsselmaterial der Trusted CA verwendet. Eine Umsignierung für E-Mails an externe Empfänger ist nicht mehr notwendig. Die Umverschlüsselung an externe Empfänger findet wieder an der Appliance nach dem „best effort“ Prinzip statt.

Da das Umsetzen dieses Konzeptes stark von der Kunden-Infrastruktur abhängig ist, wird an dieser Stelle auf eine schematisch Darstellung verzichtet.
Vorteil dieser Lösung ist eine vollständige Integration in das Kundensystem. Allerdings ist der Planungs- und Realisierungsaufwand etwas höher.
Sollte hier eine grössere Infrastruktur mit eigener PKI und/oder weiterer Sicherheitsmechanismen geplant sein, kann gegebenenfalls einer unserer Partner ein entsprechendes Gesamtkonzept mit eigener PKI anbieten.

© 2015 SEPPmail AG

### 3.5.3 Self Service Password Management (SSPM)

Das Self Service Passwort Management (kurz SSPM) ermöglicht es GINA-Benutzern selbständig Ihr Passwort zurückzusetzen. Damit werden ressourcen- und somit kostenintensive Hotline Anfragen grösstenteils vermieden.
Dabei stehen zwei Varianten zur Verfügung, um die zwei Faktoren Authentifizierung zu gewährleisten:

a) Passwortreset per SMS
Steht ein SMS-Dienst zur Verfügung, so kann sich der GINA-Benutzer nach dem Beantworten seiner persönlichen Sicherheitfrage (siehe **GINA Webmail** 23) ein Einmalpasswort bequem per SMS zusenden lassen.

b) Passwortreset per E-Mail Verifikation
Steht kein SMS-Dienst zur Verfügung oder verfügt der Benutzer über keine Gelegenheit SMS zu empfangen, so kann er sich nach dem Beantworten seiner persönlichen Sicherheitfrage und Vergabe eines neuen Passwortes von der Appliance eine E-Mail mit einem Verifikations-Link an seine hinterlegte E-Mail Adresse zusenden lassen. Nach dem Bestätigen des Links aus der E-Mail ist das Anmelden am GINA-Portal mit seinem neuen Passwort wieder möglich.

### 3.5.4 Protection Pack (VSPP)

Ein weiteres optionales Feature der SEPPmail-Appliance ist das Protection Pack, welches Virus, Spam und Phishing Schutz bietet.
Ist die Appliance aus dem Internet direkt, ohne vorgelagerte Schutzkomponenten per MX-Record zu erreichen, so empfiehlt sich der Einsatz dieser Komponente dringend, um ein Überlasten des SEPPmail- sowie der nachgelagerten Systeme aufgrund von Spam-Attacken zu vermeiden. Selbst bei vorgelagerten Schutzkomponenten ist das Scannen von verschlüsselten E-Mails auf Viren nicht möglich. Nachdem an der SEPPmail-Appliance E-Mails entschlüsselt werden, können Sie dort auch auf Viren geprüft werden. Weiterhin kann durch Aktivieren des Virenschutzes gegebenenfalls die Zweistufigkeit des selbigen gewährleistet werden.
Realisiert wird der Schutz mittels Black-, White- und Greylisting sowie der integrierten Komponenten SpamAssassin und ClamAV.

© 2015 SEPPmail AG

# 3.6 Lizenzen

## 3.6.1 Basissysteme und Lizenz

SEPPmail bietet die Basissysteme entweder als Hardware Appliance (siehe Hardwaremodelle 36) oder als virtuelle Appliance an (siehe Virtualisierte Versionen 37).
Die eingesetzte Firmware ist auf beiden Systemen identisch. Somit sind auch gemischte (Cluster-) Systeme aus physikalischen und virtuellen Appliances möglich.
Mit dem Basissystem wird auch die Basislizenz erworben, welche bereits die Domänen Verschlüsselung für das gesamte Unternehmen beinhaltet.
Weiterhin zwingend erforderlich für den Betrieb der SEPPmail-Appliance ist ein jährlicher Wartungsvertrag für das Basissystem / Lizenz.

### 3.6.1.1 Protection Pack (VSPP)

Optional kann für jede Instanz (SEPPmail-Appliance) das Protection-Pack (VSPP) gewählt werden. Der jährliche Betrag beinhaltet das Freischalten der integrierten AntiSpam sowie AntiVirus Funktionalität.
Diese Funktionalitäten werden durch verschiedene Filtermechanismen sowie dem Einsatz der Produkte SpamAssassin und ClamAV realisiert, deren Integration in den jeweils aktuellen Versionen gewährleistet wird.

**Hinweis:**
Für Systeme welche ohne vorgelagerte Schutzkomponenten direkt mit dem Internet kommunizieren, wird das Protection Pack dringend empfohlen. Andernfalls gilt es den gegebenenfalls durch Spam E-Mails zusätzlichen Ressourcenverbrauch beim Dimensionieren des SEPPmail-Systems zu beachten!

Schritt 1 zur passenden Lizenz:
Auswahl der gewünschten Appliance(s) für das Basissystem und die dazugehörige jährliche Wartung. Optional kann pro Basissystem das jährlich fällig werdende Protection-Pack (VSPP) erworben werden.

## 3.6.2 Signatur und Verschlüsselung

Soll das kryptographische Behandeln von E-Mails an der SEPPmail-Appliance auf Benutzerebene stattfinden, so ist für jede SENDENDE E-MAIL ADRESSE - unabhängig vom kryptographischen Verfahren - eine User-Lizenz zu erwerben.
Das impliziert natürlich, dass auch nur diese Nutzer verschlüsselte E-Mails über die SEPPmail-Appliance entschlüsseln können. Denn nur für diese Benutzer wird auf der Appliance das benötigte, benutzerbezogene Schlüsselmaterial gespeichert.
Diese benutzerbezogenen Lizenzen sind fest an die E-Mail Adresse des Benutzers gebunden und werden nur dann wieder freigestellt, wenn die E-Mail Adresse stillgelegt wird, zum Beispiel wenn der Mitarbeiter das Unternehmen verlässt. Werden E-Mails von einer auf der Appliance stillgelegten E-Mail Adresse versendet, so werden diese weder signiert noch verschlüsselt (auch nicht über die Domänen Verschlüsselung!). Sollte aber diese E-Mail Adresse und damit auch die allgemein gültige Domänen Verschlüsselung (ohne S/MIME, openPGP und GINA), weiter aktiv bleiben, ist das nur durch das vollständige Löschen des Users auf der SEPPmail-Appliance möglich. Wurde diesem User eigenes Schlüsselmaterial (self-signed oder offizielle Zertifikate) zugewiesen, so werden diese zunächst revoziert und anschliessend gelöscht. Über das Revozieren der Zertifikate wird den externen Kommunikationspartnern in der Regel automatisiert, das ein Verschlüsseln an die entsprechende E-Mail Adresse - anders als beim blossen Stillegen - nicht mehr möglich ist.

© 2015 SEPPmail AG

Schritt 2 zur passenden Lizenz:

Auswahl der Anzahl benötigter Signatur- und Verschlüsselungslizenzen (pro sendender E-Mail Adresse), zuzüglich dem zwingend erforderlichen, jährlichen SW Care Pack.

### 3.6.3 Large File Management (LFM)

LFM Lizenzen können in unterschiedlichen Mengen zu den Signatur- und Verschlüsselungslizenzen bezogen werden. Somit ist auch ein Betrieb der SEPPmail-Appliance als alleinstehende Lösung für den sicheren Austausch von grossen Dateien möglich.
Bei LFM handelt es sich um concurrent Lizenzen. Das heisst mit dem versenden eine übergrossen E-Mail wird der Absender E-Mail Adresse eine LFM-Lizenz zugeteilt. Versendet dieser Absender innerhalb 30 Tagen keine weitere LFM E-Mail, so wird die Lizenz automatisch wieder freigestellt.

Schritt 3 zur passenden Lizenz:

Auswahl der Anzahl gewünschter LFM-Lizenzen, zuzüglich dem zwingend erforderlichen, jährlichen LFM Care Pack.

### 3.6.4 Self Service Password Management (SSPM)

Die unter Self Service Password Management (SSPM) 56 erläuterte Funktion des SSPM, ist als einmalige, optionale Erweiterung der Signatur- und Verschlüsselungslizenz zu erwerben. Dieses Modul erhöht nicht den jährlichen Wartungsbeitrag der Care Packs.

Schritt 4 zur passenden Lizenz:

Auswahl von SSPM Lizenzen in der selben Anzahl wie Signatur- und Verschlüsselungslizenzen, sofern dieses Modul gewünscht wird.

### 3.6.5 Internal Mail Encryption (IME)

Die unter Internal Mail Encryption (IME) 53 erläuterte Lösungserweiterung zur internen Mail Verschlüsselung (IME), ist wie dasSSPM Modul ebenfalls ohne jährliche Wartung einmalig pro Signatur- und
Verschlüsselungslizenz zu erwerben.

Schritt 5 zur passenden Lizenz:

Auswahl von IME Lizenzen in der selben Anzahl wie Signatur- und Verschlüsselungslizenzen, sofern dieses Modul gewünscht wird.

© 2015 SEPPmail AG

# 4 Inbetriebnahme der Secure E-Mail-Gateway-Appliance

## 4.1 Bevor Sie beginnen

Bitte überprüfen Sie den Verpackungsinhalt auf Vollständigkeit. Der Lieferumfang besteht aus:

| Anzahl | Beschreibung |
|---|---|
| **1** | SEPPmail-Hardware-Appliance bzw. SEPPmail-Virtual-Appliance für VMware ESX oder Microsoft Hyper-V Server |
| **1** | Quick Install Guide |
| **1** | Kaltgerätekabel (240V) |

Sollte der Lieferumfang bei Ihnen unvollständig sein oder sollten bei der Installation der SEPPmail-Appliance Probleme oder Fragen auftauchen, kontaktieren Sie bitte SEPPmail oder Ihren SEPPmail Fachhändler.

Eine Liste mit den Kontaktangaben der jeweiligen Fachhändler auf der Webseite der SEPPmail AG - http://www.seppmail.ch zu finden.

© 2015 SEPPmail AG

## 4.2 Integration der SEPPmail-Appliance in Ihre E-Mail-Umgebung (Standard Konfiguration)

In diesem Abschnitt wird ein einfaches Szenario beschrieben, in dem die SEPPmail-Appliance externe E-Mails aus dem Internet direkt entgegennimmt und interne E-Mails nach extern ins Internet versendet. Je nach Aufbau Ihrer E-Mail-Infrastruktur können weitere E-Mail-Server oder Gateways im E-Mail-Datenfluss vorkommen.

In diesem Szenario wird SEPPmail als SMTP-Gateway zwischen dem Internet und dem internen E-Mail-Server installiert. Dadurch ändert sich der E-Mail-Datenfluss in den folgenden zwei wesentlichen Punkten:

1. **E-Mails aus dem Internet werden nicht mehr direkt an internen Ihren E-Mail-Server, sondern (neu) an die SEPPmail-Appliance gesendet.**

2. **Der E-Mail-Server schickt seine E-Mails nicht mehr direkt ins Internet, sondern (neu) an die SEPPmail-Appliance. Die SEPPmail-Appliance übernimmt somit eine Smarthost-Funktion.**

Die E-Mail-Infrastruktur für den beschriebenen Aufbau ist in nachfolgender Abbildung zu sehen.

**Typischer Aufbau einer E-Mail-Infrastruktur mit einer SEPPmail Appliance**

© 2015 SEPPmail AG

## 4.3 Benötigte Informationen zur Inbetriebnahme

Es wird empfohlen, folgende Informationen Ihrer E-Mail-Umgebung vor dem Inbetriebnehmen der SEPPmail-Appliance bereitzustellen:

| Benötigte Information | Ihre Angabe |
|---|---|
| **Öffentlicher DNS-Eintrag oder öffentliche IP-Adresse der Appliance*:** Name oder die IP-Adresse, unter welchem Ihre SEPPmail-Appliance aus dem Internet erreichbar sein wird. | |
| **Interne IP-Adresse der Appliance:** Interne IP-Adresse und Subnetzmaske, unter welcher die SEPPmail-Appliance im internen Netzwerk erreichbar sein wird. | |
| **Hostname der Appliance:** Frei wählbarer Hostname Ihrer SEPPmail-Appliance, zum Beispiel secureemailgateway. Dieser ist normalerweise im DNS Server aufgeführt. **Diese Einstellung entspricht der internen Sicht. Sie muss also nicht den Daten, wie sie vom Internet her Gültigkeit haben, entsprechen.** | |
| **Interne Domäne:** Beispiele sind: ihrefirma.local oder ihredomain.de usw. **Diese Einstellung entspricht der internen Sicht. Sie muss also nicht den Daten, wie sie vom Internet her Gültigkeit haben, entsprechen.** | |
| **Standard Gateway IP-Adresse:** Standard-Gateway IP-Adresse Ihrer Firewall oder Ihres Routers, über welche die SEPPmail-Appliance die Verbindung mit dem Internet herstellen kann. | |
| **DNS Server:** Die Eingabe von bis zu drei IP-Adressen von DNS-Servern ist möglich. Dabei kann es sich sowohl um externe, als auch interne DNS-Server handeln. Werden interne DNS-Server verwendet, so müssen diese Anfragen für externe Adressen entsprechend weiterleiten. | |
| **Hostname oder IP-Adresse des bestehenden internen E-Mail-Servers:** Hostname oder IP-Adresse, unter der Ihr bestehender interner E-Mail-Server im internen Netzwerk angesprochen werden kann. | |
| **E-Mail-Domänen:** Domänen der E-Mail-Adressen Ihrer Organisation an, zum Beispiel firma.ch, firma.com | |
| **Postmaster Adresse** An diese Adresse werden Systembenachrichtungen gesendet (zum Beispiel Watchdog Meldungen) | |
| **Admin E-Mail Adresse(n)** Wird für den Empfang von Passwort Rücksetzungsanfragen von GINA-Benutzern benötigt. Werden mehrere GINA Interfaces verwendet, so ist unter Umständen das Einrichten mehrerer Admins sinnvoll. | |

**Benötigte Informationen zum Einrichten der SEPPmail Appliance**

* Die SEPPmail-Appliance muss aus Internet als Webserver erreichbar sein und benötigt deshalb eine von extern erreichbare IP-Adresse. Oft ist dies die Adresse der Firewall oder eines Reverse-Proxies /

© 2015 SEPPmail AG

Web-Application-Firewall. In einfachen Installationen kann dazu die IP-Adresse verwendet werden, unter der Ihr Internet-Router von extern erreichbar ist.

Diese Information sind wie folgt herauszufinden:

1. Öffnen der Eingabeaufforderung auf einem Windows-PC
2. Eingabe des Befehls "**nslookup**" und mit "Enter" bestätigen
3. Es erscheint "**>**" Zeichen (Prompt)
4. Eingabe des Befehls "**set querytype=mx**" und mit "Enter" bestätigen
5. Eingabe der E-Mail-Domäne der eigenen Organisation (zum Beispiel ihredomain.com) und mit "Enter" bestätigen
6. Alle verfügbaren E-Mail Server werden als **"mail exchanger ="** angezeigt

Servernamen hinter dem Begriff **"mail exchanger"** mit der geringsten MX-Preference-Nummer haben die höchste Priorität bei der Namensauflösung.

© 2015 SEPPmail AG

## 4.4 Firewall / Router einrichten

Für eine korrekte Funktion der SEPPmail-Appliance sind folgende Kommunikationswege zu gewährleisten:

| Port | Quelle | Ziel | Beschreibung | |
|---|---|---|---|---|
| TCP 22 (SSH) | Appliance | update.seppmail.ch support.seppmail.ch | Wird für Updates und Lizenzänderungen der Appliance sowie dem Managed Domain Service benötigt. Weiterhin das benutzerinitiierte Öffnen von Support Sitzungen ermöglicht. Sollte der Zugriff über Port 22 nicht möglich sein, so besteht die Möglichkeit die Verbindung über einen Proxy Server herzustellen (siehe auch System 119 Proxy Settings) | |
| | Appliance | Appliance | Wird für die Synchronisation von Appliances im Clusterverbund benötigt. | ** |
| TCP 25 (SMTP) | E-Mail-Server | Appliance | Wird für den Versand ausgehender E-Mails vom internen E-Mail-Server an die SEPPmail-Appliance benötigt | ** |
| | Appliance | E-Mail-Server | Wird für den Versand eingehender E-Mails von der SEPPmail-Appliance an den internen E-Mail-Server benötigt | ** |
| | Internet | Appliance | Wird für den direkten Empfang von E-Mails aus dem Internet benötigt | |
| | Smarthost | | Wird für den Empfang von E-Mails über einen Smarthost benötigt | ** |
| | Appliance | Internet | Wird für den direkten Versand von E-Mails aus dem Internet benötigt | |
| | | Smarthost | Wird für den Versand von E-Mails über einen Smarthost benötigt | ** |
| TCP/ UDP 53 (DNS) | Appliance | Nameserver (intern) | Ermöglicht die Namensauflösung über einen/ mehrere interne DNS-Server | ** |
| | | Nameserver (extern) | Ermöglicht die Namensauflösung über einen/ mehrere externe DNS-Server | |
| | | Internet | Ermöglicht die Namensauflösung für die Einstellung **built-in DNS Resolver** | |
| TCP 80/2703 UDP 24441 | Appliance | Internet | Wird für Updates des Protection Packs (Virus, SPAM and Phishing Protection )benötigt. | * |
| TCP/ UDP 123 (NTP) | Appliance | Internet | Wird für die Zeitsynchronisation mit Zeitservern im Internet benötigt | |
| | | Timeserver (intern) | Wird für die Zeitsynchronisation mit internen Zeitservern benötigt | |
| TCP/ UDP 389 (LDAP) | Appliance | Internet | Ermöglicht LDAP Abfragen an LDAP-Server im Internet welche zum Beispiel von vielen CAs zur Bereitstellung von öffentlichen Schlüsseln betrieben werden. | * |

© 2015 SEPPmail AG

| Port | Quelle | Ziel | Beschreibung | |
|---|---|---|---|---|
| und/oder TCP/ UDP 636 (LDAPS) | | LDAP-Server (intern) | Ermöglicht LDAP Abfragen an interne LDAP-Server zur Abfrage von öffentlichen Schlüsseln interner Benutzer zum Beispiel für Interne Mail Verschlüsselung (IME). | ** |
| TCP/ UDP 388,387 (LDAP) und/oder TCP/ UDP 635 (LDAPS) | internes Netz | Appliance | Ermöglicht LDAP Abfragen an den in die Appliance integrierten Keyserver zur Abfrage von öffentlichen Schlüsseln interner Benutzer zum Beispiel für Interne Mail Verschlüsselung (IME) **oder** zur Abfrage von auf der Appliance gespeicherten öffentlicher Schlüssel von externen Kommunikationspartnern zum Beispiel für eine End-to-End Verschlüsselung. | ** |
| | Internet | | Ermöglicht LDAP Abfragen an den in die Appliance integrierten Keyserver zur Abfrage von öffentlichen Schlüsseln interner Benutzer.<br> **Hinweis**<br>Diese Freischaltung sollte aus Sicherheitsgründen nicht vorgenommen werden, da sie ein Address-Harvesting ermöglicht | * |
| TCP 443 (HTTPS) | Internet | Appliance | Wird für das Herstellen der SSL verschlüsselten Kommunikation über HTTPS zur SEPPmail-Appliance benötigt, welche für die Nutzung der GINA-Technologie verwendet wird. | |
| TCP 8080 (HTTP) und/oder TCP 8443 (HTTPS) | Admin PC | Appliance | Wird für den Zugriff auf die web-basierte Administrationsoberfläche benötigt.<br>Es wird empfohlen, nur die SSL-verschlüsselte Verbindung (HTTPS) über Port TCP/8443 zuzulassen. | ** |
| TCP 5061 | Appliance | Internet | Wird wird von vielen SMS-Gateways für den SMS-Versand via Internet verwendet. Im Bedarfsfall ist der korrekte Port direkt beim Anbieter zu erfragen. | * |

**Regeln zur Gewährleistung der Netzwerkkommunikation der SEPPmail Appliance**

* optional, je nach Konfiguration der SEPPmail-Appliance
** In einfachen Installationen wird keine Firewall zwischen der SEPPmail-Appliance und dem internen Netz verwendet. Die mit ** markierten Regeln entfallen dann.

© 2015 SEPPmail AG

## 4.5 SEPPmail-Appliance anschliessen

Falls eine virtuelle SEPPmail-Appliance erworben wurde, so ist das Image in das Host-System zu integrieren und anschliessend zu starten.
Virtuelle Abbilder stehen als OVF-Image für die Hostsysteme ESX, VMware, und RedHat HyperVisor, sowie als VHD-Image für Microsoft Hyper-V zur Verfügung.

Wurde eine Hardware Appliance erworben, so sind folgende Schritte erforderlich:

1. Verbinden der mit **LAN1** oder **eth0** gekennzeichnete Ethernet-Schnittstelle der SEPPmail-Appliance mit der Ethernet-Schnittstelle eines Computers. Je nach Hardwareausstattung und Einstellung der Schnittstellen beider Geräte, muss für diese Art der Verbindung gegebenenfalls ein gekreuztes RJ45 Patchkabel (auch bekannt als Crossover-Kabel) verwendet werden. Alternativ kann die Verbindung über einen Ethernet-Hub oder Switch mit "normalen" RJ45 Patchkabeln hergestellt werden.

2. Anschliessen der Appliance mittels beiliegendem Stromkabel an das Stromnetz.

© 2015 SEPPmail AG

## 4.6 Basiskonfiguration in wenigen Schritten

Dieses Kapitel beschreibt, wie in wenigen Schritten die Basis-Konfiguration des SEPPmail-Systems vorgenommen wird.

### 4.6.1 Netzwerkeinstellungen und Systemregistrierung

Nachfolgend wird das Integrieren der SEPPmail Appliance in die vorhandene Infrastruktur beschrieben.
Hierfür werden die in Benötigte Informationen zur Inbetriebnahme 61 gesammelten Informationen benötigt.

#### 4.6.1.1 Initialer Verbindugsaufbau

In den kommenden Abschnitten wird sowohl der initiale Zugang zu einer Hardware Appliance 66 wie auch Virtuellen Appliance 67 beschrieben. Ziel ist das initiale erreichen der Webbrowser basierten Administrationsoberfläche, über welche ausnahmslos die weitere Konfiguration erfolgt.

##### 4.6.1.1.1 Hardware Appliance

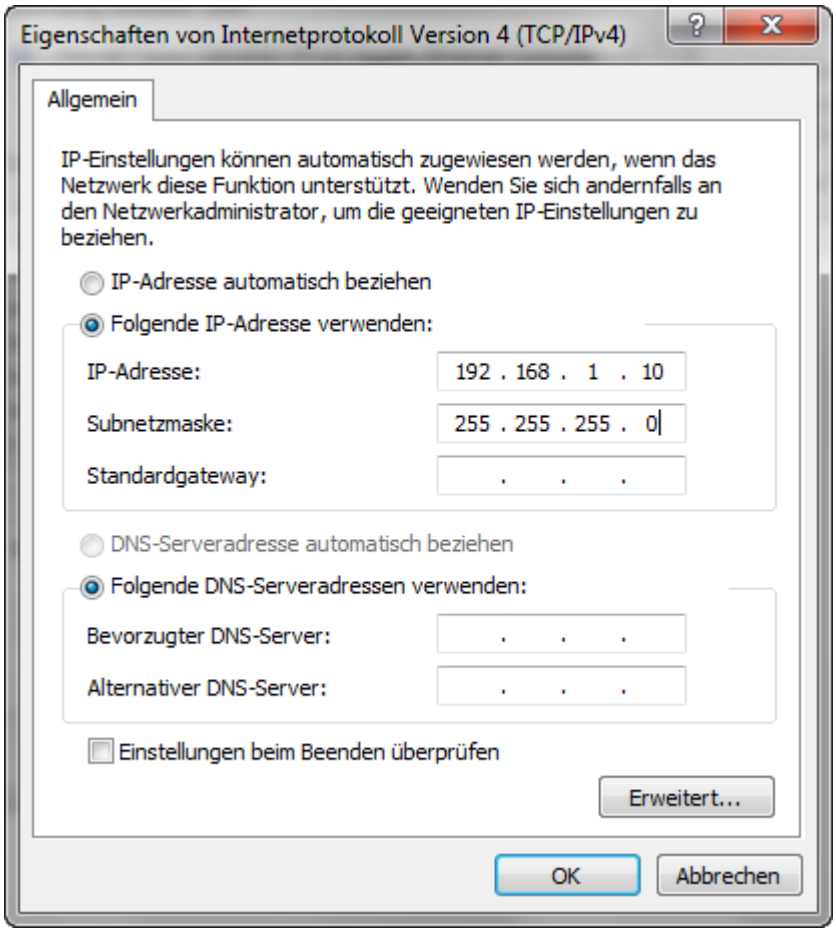
Zur erstmaligen Konfiguration der Netzwerkparameter der SEPPmail-Hardware-Appliance besteht die Möglichkeit einen Bildschirm und Tastatur anzuschliessen und die IP-Adresse temporär an der Console auf den gewünschten Wert zu ändern. Das weitere Vorgehen für dies Methode ist im Punkt Consolen Login 68 beschrieben.

Alternativ kann die SEPPmail-Hardware-Appliance über ein Crossover-Kabel oder über einen Hub direkt mit einem Computer verbunden werden.
Hierfür müssen sich beide Geräte im gleichen IP Subnetz befinden. Gegebenefall muss hierfür die IP-Adresse des Computers auf eine IP-Adresse zwischen 192.168.1.1/24 - 192.168.1.254/24, Netwerkmaske 255.255.255.0 geändert werden.

**Hinweis:**
Die Adresse 192.168.1.60 ist bereits für die SEPPmail-Appliance reserviert. Dies ist die Standard IP-Adresse im Auslieferungszustand.

Beispiel einer entsprechenden Netzwerkeinstellung anhand der Windows Oberfläche

© 2015 SEPPmail AG


Eigenschaften von Internetprotokoll Version 4 (TCP/IPv4)
Allgemein
IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.
IP-Adresse automatisch beziehen
Folgende IP-Adresse verwenden:
IP-Adresse: 192 . 168 . 1 . 10
Subnetzmaske: 255 . 255 . 255 . 0
Standardgateway:
DNS-Serveradresse automatisch beziehen
Folgende DNS-Serveradressen verwenden:
Bevorzugter DNS-Server:
Alternativer DNS-Server:
Einstellungen beim Beenden überprüfen
Erweitert...
OK
Abbrechen

Das weitere Vorgehen ist im Punkt **Login als Administrator** 70 beschrieben.

#### 4.6.1.1.2 Virtuelle Appliance

Bei einer virtuellen Appliance ist das Consolen Fenster des erstmalig gestarteten SEPPmail-Images auf dem Host-System zu öffnen.
Im Anschluss ist wie in Punkt **Consolen Login** 68 beschrieben vorzugehen.

© 2015 SEPPmail AG

#### 4.6.1.1.3 Consolen Login

Ist die SEPPmail-Appliance fertig hochgefahren, so erscheint ein Login Prompt:

```
*** Starting SEPPmail system ***
Constant subroutine Category::Ruleset::CONFBASE redefined at /usr/libdata/perl5/
Exporter.pm line 64.
 at /usr/local/sepp/GUI/Category/Ruleset.pm line 30
Nologin-Ifconfig-Hostname-Route-Nameserver-Clock-Syslog-Cluster-LDAP-License-Com
ment-Templates-Ruleset-Proxy-snmp-Loadbalance-Fetchmail-GUI-Statistics-Backup-Fi
rmware-Importldif-Restore-CA-ExternalCA-Webmail-Postfix-Daemons-DBMIG...PGP...do
ne


*******************************************************************************
***   INITIAL SETUP: Login with admin/admin to set a temporary IP address   ****
***   Login with admin/admin to set a temporary IP address                  ****
*******************************************************************************


OpenBSD/i386 (SECUREMAIL.) (ttyC0)

login: _
```

Nach der Anmeldung mit

Standard-Benutzername: admin
Standard-Kennwort: admin

wird zur Eingabe der IP-Adresse ( in diesem Beispiel 172.16.161.50 ) aufgefordert

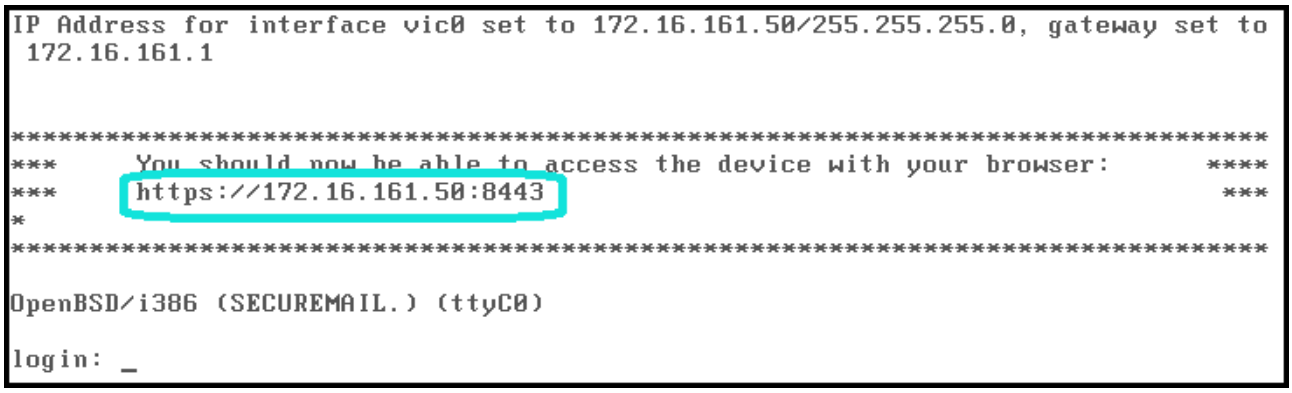
```
*******************************************************************************
***     You can now enter basic network settings. These settings are        ****
***     only temporary: You must access the Web GUI and adjust them         ****
***     under 'system' to make them permanent.                              ****
*******************************************************************************

Enter an IP address (e.g. 192.168.1.60): _
```

Weiterhin ist das Subnetz ( in diesem Beispiel 255.255.255.0 ) und Gateway Adresse ( in diesem Beispiel 172.16.161.1 ) einzugeben

```
*******************************************************************************
***     You can now enter basic network settings. These settings are        ****
***     only temporary: You must access the Web GUI and adjust them         ****
***     under 'system' to make them permanent.                              ****
*******************************************************************************

Enter an IP address (e.g. 192.168.1.60): 172.16.161.50
Enter a network mask (e.g. 255.255.255.0): 255.255.255.0
Enter the default gateway (e.g. 192.168.1.1): 172.16.161.1_
```

Abschliessend wird die URL für das Administrator Login angezeigt:

© 2015 SEPPmail AG


IP Address for interface vic0 set to 172.16.161.50/255.255.255.0, gateway set to
172.16.161.1
You should now be able to access the device with your browser:
https://172.16.161.50:8443
OpenBSD/i386 (SECUREMAIL.) (ttyC0)
login: _

Nun ist das Web-Administrationsportal der SEPPmail-Appliance - bis zum Reboot - über die angezeigte URL im Browser zu erreichen ( siehe Login als Administrator 70 )

© 2015 SEPPmail AG

#### 4.6.1.2 Login als Administrator

Sämtliche Verwaltungsmöglichkeiten der SEPPmail-Appliance stehen über eine Webbrowser basierte Konfigurationsoberfläche zur Verfügung.
Im Auslieferungszustand kann die Konfigurationsoberfläche wie folgt erreicht werden:

- Hardware Appliance über CrossOver Kabel oder Hub:

  LAN1 - https://192.168.1.60:8443
  LAN2 - https://192.168.2.60:8443

- virtuelle und Hardware Appliances, bei welchen die IP-Adresse über die Console geändert wurde:

  LAN1 - https://<Ihre temporär vergebene IP>:8443
  (siehe Login als Administrator 70)

Der Standard-Benutzername lautet: admin
Das Standard-Kennwort lautet: admin

**Hinweis:**
Erst durch die Registrierung der SEPPmail-Appliance wird eine temporäre, 30-tägeige Testlizenz bezogen beziehungsweise eine bereits vorhandene Kauflizenz aktiviert. (siehe Das System registrieren 72).
Nach erfolgreichem Registrierungsprozess verschwindet die Meldung **No valid license found - Please obtain a valid license.**

Bei Aufruf der Konfigurationsoberfläche im Webbrowser erschenit eine Warnung, dass die Webseite unsicher sei. Der Aufruf der Seite muss trotz dieser Meldung fortgesetzt werden.

**Hinweis:**
Die Meldung erscheint in der Regel nur bis ein gültiges SSL-Zertifikat installiert wurde (siehe Menüpunkt SSL 179).

#### 4.6.1.3 Netzwerkeinstellungen der SEPPmail-Appliance

Um die Netzwerkparameter der SEPPmail Appliance permanent zu konfigurieren, müssen diese in der Konfigurationsoberfläche unter dem Menüpunkt **System** eingetragen und gesichert werden.

In der **Sektion** IP Addresses
ist für das Interface 1 die IP-Adresse und die zugehörige Subnetzmaske gemäss des vorhanden Netzwerkes einzugeben

**Hnweis:**
Die Definition der Netzmaske wird nach der Classless Inter-Domain Routing (CIDR) Notation festgelegt.
- Die Netzmaske 255.255.255.255 entspricht "/32" (einzelne IP-Adresse)
- Die Netzmaske 255.255.255.0 entspricht "/24" (Klasse-C Netzwerk)
- Die Netzmaske 255.255.0.0 entspricht "/16" (Klasse-B Netzwerk)
- Die Netzmaske 255.0.0.0 entspricht "/8" (Klasse-A Netzwerk)

© 2015 SEPPmail AG

In der **Sektion** Name
sind die Felder Hostname und Domain zu füllen.
Dabei ist der Hostname ist frei wählbar, zum Beispiel securemailgateway. Der Domain-Name entspricht der DNS-Domain, in welcher sich die Appliance befindet (zum Beispiel ihrefirma.local oder ihredomain.com).
**Diese Einstellungen sind die interne Sicht, sie müssen also nicht den Daten, wie sie vom Internet her Gültigkeit hätten, entsprechen.**

In der **Sektion** DNS
kann zwischen der Verwendung der Root-DNS-Server im Internet (**Use built-in DNS Resolver**) oder eines explizit anzugebenden DNS-Server gewählt werden (**Use the following DNS Servers**)
Wird die Einstellung **Use built-in DNS Resolver** verwendet, kann das Auflösen von Namen unter Umständen etwas länger dauern, wodurch die Performanz des Systems beeinträchtigt werden kann.
Bei Angabe eines DNS-Servers (Primary) ist darauf zu achten, dass dieser auch Domänen Namen im Internet auflösen kann. Falsche Einträge können zu einem sehr langsamen Antwortverhalten der Konfigurationsoberfläche sowie Problemen bei der Kommunikation mit Drittsystemen führen. Über die Eingabefelder Alternate1 und Alternate 2 können bei Bedarf weitere, alternative DNS Server eingegeben werden. Dadurch würde bei Ausfall des "Primary" Servers würde der "Alternate 1" übernehmen, sollte auch dieser ausfallen der "Alternate 2".

In der **Sektion** Routing
wird das zum Subnetz passende Default Gateway eingetragen. Diese Eingabe wird benötigt um Netze ausserhalb des Eigenen zu erreichen.

Eine detaillierte Beschreibung der einzelnen Sektionen ist im Menüpunkt System 119 zu finden.

#### 4.6.1.4 Netzwerkkonfiguration prüfen

Um sicherzustellen, dass die vorgenommenen Netzwerkeinstellungen der SEPPmail-Appliance korrekt sind, ist in der Konfigurationsoberfläche unter dem Menüpunkt **Administration** im Punkt Update auf die Schaltfläche **Check for update** zu klicken.

Falls eine der beiden folgenden Meldungen erscheint,

- **You already have the latest version installed**
- **There is a new version available: Installed version is *alteVersionsnummer*, latest version is *neueVersionsnummer***

war die Netzwerkkonfiguration erfolgreich.

Erscheint die Meldung

- **ERROR: unable to connect to update server. Make sure that the device can make connections to the internet on port 22**.

ist eine Verbindung in das Internet über Port TCP/22 (SSH) nicht möglich. Die Netzwerkeinstellungen der SEPPmail-Appliance sowie die Firewall- bzw. Router-Einstellungen sind erneut zu prüfen (siehe Firewall / Router einrichten 63).

Eine detaillierte Beschreibung zum Update ist unter Administration 190 zu finden.

© 2015 SEPPmail AG

#### 4.6.1.5 Das System registrieren

Das Registrieren des SEPPmail-Systems erfolgt im Web-Administrationsportal unter dem Menüpunkt **Administration** **License and registration** durch wählen der Schaltfläche **Register this device...**.

Mit dem Registrieren der Appliance

- bezieht das System eine 30-tägige Testlizenz
- wird bei Eingabe des Activation code am Ende der Registrierungsseite eine Kauflizenz aktiviert. Der Activation Code entspricht der License-ID (xxxx-xxxx-xxxx) auf dem **"SEPPmail License Certificate"**.

Erscheint die Meldung Registration successful, so wurde der Registrierungsvorgang erfolgreich abgeschlossen.

Eine detaillierte Beschreibung der einzelnen Vorgänge ist im Kapitel **Register this device** 193 zu finden.

### 4.6.2 Das System auf den neusten Stand bringen

Im Unterpunkt **Update** des Menüpunktes **Administration** sind die verschiedenen Update Optionen zu finden.

Ist die SEPPmail-Appliance bereits auf dem aktuellen Stand, so ist die Meldung

> **You already have the latest version installed**

zu sehen. Andernfalls wird die aktuell auf der SEPPmail-Appliance installierte, sowie die auf dem Update-Server bereitgestellte Version angezeigt

> **There is a new version available: Installed version is *alteVersionsnummer*, latest version is *neueVersionsnummer***

In diesem Fall ist die Appliance so oft über die Schaltfläche **Fetch update** zu aktualisieren, bis die Meldung **"You already have the latest version installed"** erscheint (siehe **Administration** 190).
Durch erneutes Klicken auf die Schaltfläche **Fetch update** wird gegebenenfalls der Update-Fortschritt in % angezeigt.
Nach jedem Update erfolgt ein Neustart der SEPPmail-Appliance.

© 2015 SEPPmail AG

### 4.6.3 Wichtige Sicherheitsmassnahmen

In den kommenden Abschnitten werden folgende Sicherheitsmassnahmen beschrieben:

- Ändern des Administrator-Passworts 73
- Festlegen des HTTPS-Protokolls für den sicheren Zugriff auf die Appliance 73
- Erstellen eines Backup Users zur regelmässigen Sicherung der Appliance 73
- Eingabe der Postmaster Adresse für den Empfang von Systemmeldungen 74

#### 4.6.3.1 Administrator-Kennwort ändern

Aus Sicherheitsgründen sollte das Kennwort des Benutzers admin unbedingt geändert und auf einen entsprechend komplexen Wert gesetzt werden.

Das Ändern des Passwortes kann sowohl über das Menü **Login** im Punkt **Change Password** (siehe Menüpunkt **Login** 115) als auch den Benutzerdetails des Benutzers "admin" im Menü **Users** (siehe **Benutzerdetails** 204 **User Data** Password) erfolgen.

#### 4.6.3.2 Festlegen des HTTPS-Protokolls für den sicheren Zugriff zum System

Im Menüpunkt **System** sind nach dem Klicken der Schaltfläche **Advanced view** weitere Konfigurationsoptionen sichtbar. In den Sektionen **GUI protocol** und **GINA https protocol** werden die Zugriffsoptionen auf die Appliance (HTTP oder HTTPS) eingestellt.

Aus Sicherheitsgründen wird empfohlen, die Option HTTP zu deaktivieren und sowohl für die Konfigurationsoberfläche **GUI protocol** wie auch für **GINA https protocol** nur HTTPS zuzulassen. Das ungesicherte HTTP-Protokoll sollte nur dann Verwendung finden, wenn bereits eine vorgelagerte Komponente den SSL-Tunnel terminiert und die Verbindung zwischen dieser Komponente und der SEPPmail-Appliance über ein gesichertes Netzwerk stattfindet.

Eine detaillierte Beschreibung der einzelnen Sektionen ist im Menüpunkt **System** 119 zu finden.

#### 4.6.3.3 Backup Benutzer erstellen

Der Backup Prozess der SEPPmail-Appliance erstellt täglich automatisiert eine Sicherung. Für die Funktion dieses Prozesses sind zwei Schritte notwendig:

1. **Backup Kennwort setzen**
   Da die Backups der Appliance grundsätzlich verschlüsselt werden, ist die Eingabe eines Backup Kennwortes zwingend. Das Setzen erfolgt unter dem Menüpunkt **Administration**, in der Sektion **Backup** mittels der Schaltfläche **Change password** (siehe **Administration** 190 **Backup**)

2. **Zuordnung eines Users zur Gruppe Backup**
   Nach dem automatischen Erstellen des Backups wird dieses an alle Mitglieder der Gruppe Backup gesendet. Das Zuordnen von Benutzern erfolgt über den Menüpunkt **Groups** in der Sektion **backup (Backup Operator)** über die Schaltfläche **Edit...** (siehe **Groups** 213 **backup (Backup Operator )**).
   Soll für diesen Zweck ein eigener Benutzer angelegt werden, so ist darauf zu achten, dass

© 2015 SEPPmail AG

dieser eine gültige E-Mail-Adresse in der beziehungsweise einer der interne E-Mail Domänen besitzt. Das ziehen einer Verschlüsselungslizenz für diesen Benutzer kann gegebenenfalls durch aktivieren der Optionen "May not encrypt mails" und "May not sign mails" unterbunden werden (siehe Benutzerdetails 204).

Da aufgrund des Aufbaus der Appliance lediglich die Maschinenkonfiguration sowie das Schlüsselmaterial gesichert werden muss, fallen die Backups extrem klein aus (< 1 MB). Dies macht den Versand per E-Mail unproblematisch.

#### 4.6.3.4 Eingabe der Postmaster Adresse für den Empfang von Systemmeldungen

Damit Benachrichtigungen des SEPPmail-Systems über eventuelle Probleme (Watchdog Meldungen) versendet werden können, ist die Eingabe einer entsprechenden E-Mail Adresse für den Empfang dieser Meldungen im Menü **Mail System** unter der Sektion **SMTP settings** in das Feld Postmaster address erforderlich.

© 2015 SEPPmail AG

## 4.7 Vorbereiten der GINA-Technologie

Um auch mit Kommunikationspartnern, welche selbst über kein Schlüsselmaterial verfügen sicher kommunizieren zu können, kommt die GINA-Technologie zum Einsatz.

Für das initiale Einrichten dieses Verfahrens ist zunächst die Erreichbarkeit der SEPPmail-Appliance aus dem Internet - in der Regel per SSL Port 443 (siehe **Firewall / Router einrichten** 63) - zu gewährleisten.
Weiterhin sollte auf der Appliance ein gültiges SSL-Zertifikat einer vertrauenswürdigen Certification Authorothy (CA) eingebunden sein (siehe **SSL** 179).
Letztendlich sind die GINA-Einstellung über **Edit GINA Settings** 165 vorzunehmen.

© 2015 SEPPmail AG

## 4.8 Integration in die bestehende E-Mail Infrastruktur

Die Basis-Einrichtung der SEPPmail-Appliance ist mit dem Abarbeiten der vorangegangenen Punkte abgeschlossen.

Für eine Minimalkonfiguration zum Austausch sicherer E-Mails sind die in den folgenden Punkten beschriebenen weiteren Schritte notwendig.

### 4.8.1 Zu verwaltende E-Mail-Domänen einrichten

Die E-Mail Domänen auf welche das neue SEPPmail-System reagieren soll, sind Menü **Mail System** Sektion **Managed Domains** über die Schaltfläche **Add Domain...** einzugeben.
Dabei wird unter Domain Name der Name der E-Mail Domäne eingegeben.
Als Forwarding Server IP or MX name wird in der Regel der Groupware Server angegeben, an welchen die E-Mails intern weitergeleitet werden (siehe auch Add/Edit Managed Domain 136).

### 4.8.2 Ausgehenden E-Mail-Verkehr steuern

Das Abgeben der ausgehenden E-mails in das Internet wird im Menü **Mail System** Sektion **Outgoing Server** gesteuert. Soll die SEPPmail-Appliance E-Mails direkt an externe E-Mail-Empfänger im Internet abgeben, so ist die Option **Use built-in mail transport agent** zu wählen. Sollte an ein vorgelagertes System weitergeleiten werden, so ist die Option **Use the following SMTP server:** zu wählen. Dann ist unter Server name der entsprechde Name oder die IP-Adresse dieses Systems einzutragen. Erfordert dieses System eine Authentifizierung, so ist der erforderlich Benutzername unter User ID und das Kennwort unter Password einzugeben (siehe auch Mail System 129 Outgoing Server).

**Hinweis:**
Bei Verwenden der Einstellung **Use built-in mail transport agent** wird dringend empfohlen das optionale Protection Pack (VSPP) zu lizensieren und aktivieren, sofern für den eingehenden E-Mail Verkehr nicht etwa ein externer AntiSpam-Dienst vorgeschaltet ist. Andernfalls ist mit erheblichen Beeinträchtigungen, bis hin zum Erliegen des Mailflusses durch SPAM-Attacken zu rechnen.

### 4.8.3 Mail Relaying

Damit das interne Groupware System in der Lage ist, ausgehende E-Mails an das SEPPmail-System abzugeben, ist es notwendig, die IP-Adresse des, beziehungsweise unter Umständen auch das Netz in dem die Groupware Server stehen zu berechtigen.
Dies erfolgt durch den Eintrag der IP(s) beziehungsweise des oder der Netze in die dafür vorgesehenen Felder des Menüs **Mail System** in der Sektion **Relaying** (siehe auch Mail System 129 Relaying).

© 2015 SEPPmail AG

## 4.8.4 SSL-Zertifikat einbinden

Eine detaillierte Beschreibung des Menüpunktes **SSL** ist unter **SSL** 179 zu finden.
Die folgenden Seiten liefern lediglich eine Kurzbeschreibung zur Inbetriebnahme.

### 4.8.4.1 SSL-Device-Zertifikat selbst erstellen

SEPPmail ermöglicht es, ein eigenes SSL-Device-Certificate über die Konfigurationsoberfläche zu erstellen. Für eine Testinstallation ist es nicht zwingend erforderlich ein kostenpflichtiges SSL-Device-Certificate zu beschaffen. Das Zertifikat kann auf der SEPPmail-Appliance automatisch generiert und signiert werden.

Hierfür ist in das Menü **SSL** zu wechseln und die Schaltfläche **Request an new Certificate...** zu klicken.

Im erscheinenden Menü sind die hier aufgeführten Felder zwingend auszufüllen:

**Sektion Issue To**

| Parameter | Beschreibung |
|---|---|
| Name or IP (CN) | IP-Adresse oder Hostname unter der SEPPmail aus dem Internet erreichbar ist. Bei einem selbstsignierten Zertifikat muss der hier angegebene Werte dem Namen in der URL entsprechen unter der SEPPmail angesprochen wird.<br>**Beispiel:**<br>Soll SEPPmail unter der URL **https://securewebmail.example.tld** angesprochen werden, so lautet der im Feld **Name or IP (CN)** anzugebende Hostname **securewebmail.example.tld.** |
| E-Mail | Eine gültige E-Mail-Adresse innerhalb der Firma, unter der eine zuständige Person erreicht werden kann. |
| Country (C) | Land, in dem die Organisation ihren Sitz hat. |

**Sektion Attributes**

| Parameter | Beschreibung |
|---|---|
| **Key size (bits)** | In der Regel ist die maximale Schlüssellänge zu wählen um den aktuellen Sicherheitsstandards zu entsprechen. |
| **Signature** | Für das Erstellen eines selbs signierten Zertifikates ist **Create self-signed certificate** auszuwählen. |

Um die Erstellung des SSL-Zertifikats auszuführen, ist auf die Schaltfläche **Create Request** zu klicken. Durch die Bestätigung mit folgenden Zertifikatsdetails

- die Seriennummer des Zertifikats **(Serial No.)**

© 2015 SEPPmail AG

- die Gültigkeitsdauer **(Validity)**
- den Fingerprint **(SHA1 Fingerprint)**

ist der Vorgang abgeschlossen.

**Hinweis:**
Auch das Erstellen eines **Wildcard SSL-Zertifikats** ist möglich. Wildcard Zertifikate gelten nicht nur für einen dedizierten Host sondern können für mehrere Hosts einer Domäne verwendet werden.

**Beispiel:**
Ein SSL-Zertifikat mit dem Namen ginatest.testdomain.net kann nur für diesen einen Host verwendet werden. Anderenfalls wird eine Zertifikatsfehlermeldung im Webbrowser angezeigt. Ein Wildcard SSL-Zertifikat können Sie auf beliebigen Hosts einer Domäne verwenden, zum Beispiel ginatest.testdomain.net, webmail.testdomain.net oder secmail.testdomain.net.

Um ein Wildcard SSL-Zertifikat zu erzeugen, geben Sie den Hostnamen mit einem führenden Stern "*" ein, zum Beispiel *.testdomain.net .

Zur Aktivierung des neuen SSL-Device-Certifikate ist ein Neustart der SEPPmail-Appliance erforderlich (siehe **Administration** **System** **Reboot System** **Reboot** beziehungsweise **Administration** 190).

Detaillierte Informationen sind unter **Request a new Certificate** 181 zu finden.

#### 4.8.4.2 SSL-Device-Zertifikat von einer öffentlichen Zertifizierungsstelle anfordern

Für den produktiven Betrieb der SEPPmail inklusive GINA-Technologie empfiehlt sich dringend das Verwenden eines Trusted-SSL-Device-Certificate für den SSL-gesicherten Zugriff auf das GINA-Webmail-System.

Für das Anfordern und anschliessende Einbinden eines gekauften Trusted-SSL-Device-Certificate ist in das Menü **SSL** zu wechseln und die Schaltfläche **Request an new Certificate...** zu klicken.

Im erscheinenden Menü sind die hier aufgeführten Felder zwingend auszufüllen:

**Sektion** **Issue To**

| Parameter | Beschreibung |
|---|---|
| Name or IP (CN) | IP-Adresse oder Hostname unter der SEPPmail aus dem Internet erreichbar ist. Bei einem selbstsignierten Zertifikat muss der hier angegebene Werte dem Namen in der URL entsprechen unter der SEPPmail angesprochen wird.<br>**Beispiel:**<br>Soll SEPPmail unter der URL **https://securewebmail.example.tld** angesprochen werden, so lautet der im Feld **Name or IP (CN)** anzugebende Hostname **securewebmail.example.tld.** |

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| E-Mail | Eine gültige E-Mail-Adresse innerhalb der Firma, unter der eine zuständige Person erreicht werden kann. |
| Country (C) | Land, in dem die Organisation ihren Sitz hat. |

**Sektion Attributes**

| Parameter | Beschreibung |
|---|---|
| **Key size (bits)** | In der Regel ist die maximale Schlüssellänge zu wählen um den aktuellen Sicherheitsstandards zu entsprechen. |
| **Signature** | Für das Anfordern eines Trusted-SSL-Device-Certificate ist **Create certificate signing request** auszuwählen. |

Um ein Schlüsselpaar zu erzeugen und den Antrag zur Signierung des öffentlichen Schlüssels (certificte signing request, kurz CSR) zu erstellen, ist auf die Schaltfläche **Create Request** zu klicken. In der Grünen Statusleiste oben im Menü erscheint danach **Certificate request created**. Ganz unten im Menü erscheint die Schaltfläche **Download and Import signed Certificate...** über welche zunächst der CSR zu finden ist. Nach dem Hochladen des CSR zur Trusted CA und dem anschliessenden Erhalt des Zertifikates, kann dieses - gegebenenfalls durch erneutes Klicken auf die Schaltfläche **Download and Import signed Certificate...**, sofern das Menü zwischenzeitlich gewechselt wurde - unter Import Certificate eingefügt und per Schaltfläche **Import Certificate** importiert werden.

**Hinweis:**
Falls im oberen Bereich des Menüs die gelb hinterlegte Information **Remember to import the signed certificate** angezeigt wird, so wurde zuvor bereits ein Zertifikatsantrag erstellt.

Das neu erstellte SSL-Device-Zertifikate sollte zusammen mit den gegebenenfalls zusätzlich benötigten Intermediate CA-Zertifikate(n) und dem Zertifikat der Root-CA selbst in der Reinhenfolge

1. Public Key des eigenen SSL-Device-Zertifikats
2. Public Key von einer oder mehreren Intermediate CA-Zertifikaten
3. Public Key der Root-CA

eingefügt werden
Im Fehlerfall ist das SSL-Device-Zertifikat nicht zu nutzen. Ebenfalls kann dies zu Problemen beim Zugriff auf die Konfigurationsoberfläche führen. Für diesen Fall sollte sicherheitshalber vor dieser Aktion temporär der HTTP-Port (siehe **System Advanced View GUIProtocol** HTTP Port) für den Zugriff auf die Administrationsoberfläche (http://<Appliance>:8080) freigegeben werden.

Zur Aktivierung des neuen SSL-Device-Certificate ist ein Neustart der SEPPmail-Appliance erforderlich (siehe **Administration System Reboot System Reboot** beziehungsweise Administration 190).

Detaillierte Informationen sind unter Request a new Certificate 181 zu finden.

© 2015 SEPPmail AG

#### 4.8.4.3 Bestehendes SSL-Device-Zertifikat verwenden

Für den produktiven Betrieb der SEPPmail inklusive GINA-Technologie empfiehlt sich dringend das Verwenden eines Trusted-SSL-Device-Certificate für den SSL-gesicherten Zugriff auf das GINA-Webmail-System.

Für das Einbinden eines gekauften Trusted-SSL-Device-Certificate ist in das Menü **SSL** zu wechseln und die Schaltfläche **Request an new Certificate...** zu klicken.

Im erscheinenden Menü ist in der Sektion **Upload existing key** das Einbinden auf zwei Arten - abhängig vom vorliegenden Zertifikats-Format (pem oder PKCS#12 also p12 oder pfx) - möglich. Dabei werden die ersten beiden Parameter ausschliesslich für die Integration des pem-Formats, die beiden letzteren Parameter für die Integration des PKCS#12-Formates benötigt.

| Parameter | Beschreibung |
|---|---|
| X.509 Key<br>Note: Remove password before uploading a key | In dieses Feld wird der Private Schlüssel aus der pem-Datei eingefügt. Hierfür wird die pem-Datei mit einem Editor geöffnet- Falls der private Schlüssel durch ein Kennwort geschützt ist, muss dieses zuvor entfernt werden. Im Anschluss wird der Private Schlüssel (dieser beginnt mit -----BEGIN PRIVATE KEY----- und endet mit -----END PRIVATE KEY-----) in das Eingabefeld kopiert.<br>**Die Eingabe muss unbedingt mit einer Leerzeile abgeschlossen werden!** |
| X.509 Certificate<br>(and optional intermediate certificates) | In dieses Feld wird der Öffentliche Schlüssel aus der pem-Datei eingefügt. Dieser ist unterhalb des Privaten Schlüssel in der pem-Datei zu finden und beginnt mit -----BEGIN CERTIFICATE----- und endet mit -----END CERTIFICATE-----.<br>Unter Umständen sind in der pem-Datei weitere Zertifikate enthalten. Dabei handelt es sich um Zwischen- oder auch Intermediate- Zertifikate, welche unterhalb des Öffentlichen Schlüssels in dieses Feld kopiert werden müssen. Zuletzt wird das Zertifikat der Root CA eingefügt.<br>**Die Eingabe muss unbedingt mit einer Leerzeile abgeschlossen werden!**<br><br>**Hinweis:**<br>**In dieses Eingabefeld sollten alle notwendigen Zwischenzertifikate für eine vollständige Zertifikatskette eingefügt werden. Eine unvollständige Zertifikatskette führt bei der Zertifikatsprüfung immer dann zu Problemen, wenn der Gegenstelle diese nicht bereits bekannt ist. Internet-Tools - wie zum Beispiel CheckTLS - zeigen dann einen falschen TLS-Status an.**<br>**Nicht jede pem-Datei enthält die komplette Zertifikatskette. In diesem Fall müssen die benötigten Zwischenzertifikate gegebenenfalls anderweitig besorgt werden.** |
| **Key and certificate in PKCS12 format** | Über die Internet-Browser Schaltfläche "Datei auswählen" wird die PKCS#12-Datei (diese hat die Endung .p12 oder .pfx) ausgewählt. |

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| | **Hinweis:**<br>**Auch hier muss darauf geachtet werden, dass diese Datei die komplette Zertifikatskette, also auch die Zwischenzertifikate enthält. Gegebenenfalls kann nach dem Import der PKCS#12 Datei ein Backup des Zertifikates (siehe SSL 179) vorgenommen werden. Die dadurch zur Verfügung stehende pem-Datei kann mit einem Editor geöffnet und anschliessend wie oben beschrieben wieder inklusive Zwischenzertifikate importiert werden.** |
| PKCS12 password | Nachdem eine PKCS#12-Datei den Privaten Schlüssel enthält, ist diese Passwort geschützt. Das Passwort muss vor dem Import der oben ausgewählten PKCS#12-Datei in dieses Eingabefeld eingegeben werden. |

Über die Schaltfläche **Upload Key and Certificate** wird das SSL-Zertifikat in die Appliance hochgeladen.
Aktiv wird das Zertifikat nach einem Neustart der Appliance.

Detaillierte Informationen sind unter **Request a new Certificate** 181 zu finden.

© 2015 SEPPmail AG

### 4.8.5 E-Mail-Datenfluss umstellen

Um den sicheren E-Mail-Verkehr mit der SEPPmail-Appliance zu ermöglichen, müssen folgende Änderungen am bestehenden E-Mail-Server vorgenommen werden:

**In das Internet:**

1. **SEPPmail-Appliance als Smarthost definieren**
   Die SEPPmail Appliance wird nach der Integration in die bestehende E-Mail-Umgebung die Rolle eines SMTP-Gateways übernehmen. Der E-Mail-Server übermittelt somit E-Mails nicht mehr direkt nach extern, beziehungsweise an das gegebenenfalls bereits vorhandene SMTP-Gateway (zum Beispiel Spam-Filter), sondern (neu) nun an die SEPPmail-Appliance.
   Um diese Änderung vorzunehmen, muss auf dem bestehenden E-Mail-Server der interne Hostname beziehungsweise IP-Adresse der SEPPmail-Appliance als **Smarthost** definiert werden.
   Auf der Appliance sind die Relaying einstellungen zu beachten (siehe Abschnitt Mail Relaying 76).

2. **Autorisieren der SEPPmail-Appliance für den E-Mail-Versand**
   a) Ist die SEPPmail-Appliance direkt mit dem Internet verbunden, so sind die korrekten Firewall- beziehungsweise Router-Einstellungen zu gewährleisten (siehe Abschnitt Firewall / Router einrichten 63).
   b) Ist der SEPPmail-Appliance zum Internet hin noch ein weiterer Smarthost (zum Beispiel ein Spam-Filter) vorgeschaltet, so ist der interne Hostname beziehungsweise die IP-Adresse der SEPPmail-Appliance auf diesem Smarthost in die Liste der autorisierten E-Mail-Relay Systeme einzutragen.
   Die Appliance ist entsprechend einzustellen (siehe Ausgehenden E-Mail Verkehr steuern 76).

**Aus dem Internet:**

1. **Umstellung des MX-Eintrages**
   War der E-Mail-Server bislang direkt mit dem Internet verbunden, so muss der vorhandene MX-Eintrag zukünftig nicht mehr auf den Hostnamen beziehungsweise die IP-Adresse des E-Mail-Servers, sondern (neu) auf die SEPPmail-Appliance zeigen.

2. **Umstellung des Smarthost**
   Nimmt ein Smarthost die E-Mails aus dem Internet entgegen und leitete diese bislang direkt an den E-Mail-Server weiter, so muss dieser die E-Mails zukünftig an die SEPPmail-Appliance abgeben.

**ACHTUNG**

**Mit dieser Anpassung wird die SEPPmail-Appliance in den E-Mail-Datenfluss integriert. Alle E-Mails werden nach der Umstellung an die SEPPmail-Appliance gesendet.**

**Das Umstellen des E-Mail-Datenflusses darf erst dann erfolgen, wenn alle anderen Konfigurationsschritte der SEPPmail-Appliance abgeschlossen sind. Andernfalls ist eine Beeinträchtigung des E-Mail-Verkehrs nicht ausgeschlossen.**

© 2015 SEPPmail AG

#### 4.8.5.1 IronPort Anbindung der SEPPmail

**Achtung:**

Wichtig ist, die aktuelle Policy des IronPort Systems zu verstehen, bevor Änderungen durchgeführt werden.

## Konfigurationsvorschlag

Alle einkommenden E-Mails werden von IronPort empfangen und auf SPAM und Viren geprüft. Alle soweit geprüften E-Mails werden an die SEPPmail-Appliance weitergeleitet, wo diese gegebenenfalls entschlüsselt und zur IronPort zurück gesendet werden. Dort werden alle E-Mails (jetzt auch die entschlüsselten) nochmals Viren und SPAM geprüft und an das interne Groupware-System, zum Beispiel MS-Exchange oder Lotus Notes, weitergeleitet.

Alternativ kann das IronPort-System veranlasst werden, verschlüsselte und/oder signierte E-Mails zu erkennen und nur diese an die SEPPmail-Appliance umleiten. Alle anderen E-Mails werden direkt an das interne Groupware-System weitergeleitet.

Ausgehende E-Mails schickt das interne Groupware-System zu IronPort. Dieses leitet ausgehende E-Mails in jedem Fall zu SEPPmail weiter. Dort wird das Regelwerk gepflegt, welche E-Mails signiert und verschlüsselt werden sollen. Anschliessend werden die ausgehenden E-Mails vom SEPPmail-System zurück zum IronPort-System geleitet, welches als einziges System E-Mails in Richtung Internet versendet.

Das Problem bei dieser Konfiguration ist, dass das SEPPmail-System in der Relayliste des IronPort-Systems stehen muss, da das SEPPmail-System ausgehende E-Mails in Richtung Internet versenden will. Für alle Hosts in der Relay-Liste von IronPort gilt automatisch immer die Outgoing Mail Policy. Nach der akutellen Outgoing Policy findet dort keine Virenprüfung statt, so dass die SEPPmail Anbindung so keinen Zusatznutzen bringt.

**Dazu gibt es zwei Lösungen:**

1. Die Outgoing Mail Policy auf dem IronPort System wird so umgebaut, dass sie ähnlich aussieht wie die Incoming Policy. Das ist aber eine unschöne Lösung.

2. Sie konfigurieren einen speziellen Listener, über den die SEPPmail-Appliance eingehende E-Mails einliefert. Auf diesem Listener darf das SEPPmail-System nicht in der Relay-Liste eingetragen sein. Dieser Listener kann zum Beispiel auf der bestehenden IP-Adresse 192.168.1.11 auf einen speziellen Port (zum Beispiel 10025) gebunden sein, oder auf einer weiteren IP-Adresse im IP-Netzwerk 192.168.1.0/24.

**Die Umleitung kann man auf zwei Arten Implementieren:**

1. per Content Filter
2. per Message Filter

Der Unterschied zwischen Message Filter und Content Filter ist, dass ein Message Filter immer auf die gesamte E-Mail angewendet wird. Hat eine E-Mail zum Beispiel mehrere Empfänger, so gilt die Aktion für alle Empfänger. Bei einem Content Filter kann man über verschiedene Policy-Einträge die E-Mail aufsplitten. Das sollte in unserem Fall keine Rolle spielen. Ein weiterer Unterschied ist, dass man im Message Filter erkennen kann, ob eine E-Mail verschlüsselt oder signiert ist und somit nur diese E-Mail zur SEPPmail-Appliance umleiten kann.

Um die Lösung einfach und übersichtlich zu gestalten empfehlen wir, alle ausgehenden E-Mails zur SEPPmail-Appliance weiterzuleiten (nicht nur die zu verschlüsselnden oder signierenden E-Mails) und mit einem Content Filter zu arbeiten.

© 2015 SEPPmail AG

## Konfiguration

### IronPort

- Bestehender Listener mit SEPPmail in der Relay-Liste
- Neuer Listener Incoming SEPPmail mit SEPPmail nicht in der Relay-Liste

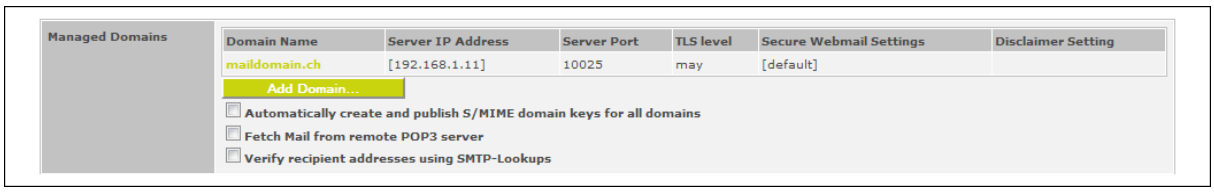
### Incoming Contentfilter : IncomingSEPPmail

```
(normalerweise nicht notwendig: Receiving Listener = IncomingMail AND)

Remote IP IS NOT \[IP von SEPPmail 1\]
AND
Remote IP IS NOT \[IP von SEPPmail 2\]

(optional, falls Sie nur eine Ihrer Domänen über SEPPmail
betreiben lassen wollen: AND Envelope Recipient
ends with @securemailcustomer.ch )

Action: Send to Alternate Destination Host: \[Cluster IP der beiden SEPPmail\]
```

### SEPPmail

Das SEPPmail System ist so einzurichten, dass eingehende E-Mails an den **Incoming SEPPmail Listener** geschickt werden.

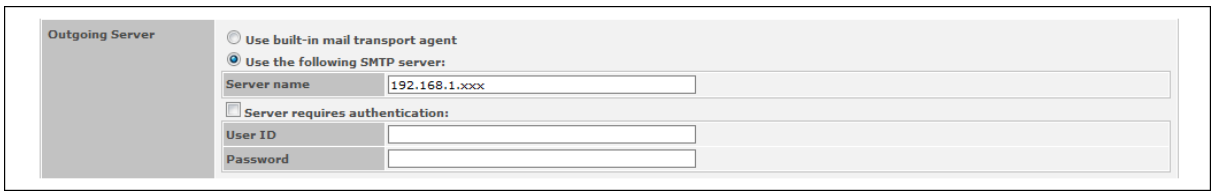
**Menü Mail System:** Siehe "Zu verwaltende E-Mail Domänen einrichten" 76.




**Sektion Managed Domains**

Das Problem hier ist, dass in der SEPPmail Konfiguration nur eine einzige IP-Adresse angegeben werden kann, wohin die eingehenden E-Mails weitergeleitet werden, also nicht beide Incoming IP-Adressen Ihrer IronPorts. Hierzu ist es notwendig, einen (fiktiven) DNS-Eintrag zu erzeugen, welcher in beide IP-Adressen der IronPorts aufgelöst werden kann. Dieser fiktive DNS-Name wird als "Server IP Address" der E-Mail-Domäne eingetragen.

Ausgehende E-Mail versendet SEPPmail an den **bestehenden Listener**:
Siehe "Ausgehenden E-Mail-Verkehr steuern" 76.



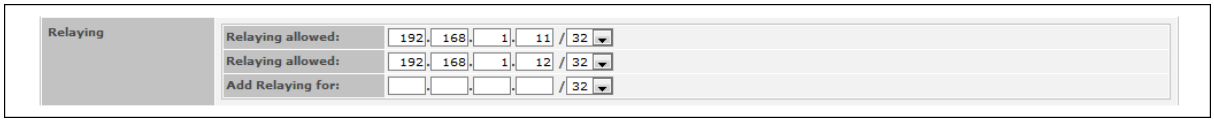

**Sektion Outgoing Server**

Hier ist die IP-Adresse des Listeners anzugeben, bzw. wie oben ein Hostname, welcher auf beide

© 2015 SEPPmail AG

Listener aufgelöst wird.

Für beide IP-Adressen der IronPort Systeme ist im SEPPmail-System die Relay-Berechtigung einzutragen. Siehe "Mail Relaying" 76.




**Sektion** Relaying

Die Konfigurationsbeschreibung für die SEPPmail - IronPort Anbindung wurde uns mit freundlicher Genehmigung zur Verfügung gestellt von:

**AVANTEC AG**
Badenerstrasse 281
CH-8003 Zürich
http://www.avantec.ch
info@avantec.ch

© 2015 SEPPmail AG

### 4.8.6 Steuern der Appliance

Die von der Appliance durchzuführenden gewünschten Aktionen - zum Beispiel Signieren und/oder Verschlüsseln - können als globale Aktion an der Appliance oder über vordefinierte Merkmale individuell am Client ausgelöst werden.

Steuerungsmerkmale sind Betreffzeilen Schlüsselworte (siehe Tabelle 1), welche bei Bedarf verändert werden können und durch welche die Unabhängigkeit vom eingesetzten E-Mail Client gewährleistet wird.
Ebenso können jedoch (X-)Header für das Ansteuern der Kryptographischen Aktionen ausgewertet werden (ebenfalls Tabelle 1).

| Betreffzeilen Schlüsselwort | (x-)header / Wert | |
|---|---|---|
| [plain] | x-smplain / yes | E-Mail mit diesem Kennzeichen durchlaufen nicht das Ruleset und werden somit kryptographisch unbehandelt versendet |
| [confidential] | sensitivity / companyconfidential x-smenc / yes | Anfordern der Verschlüsselung |
| [priv] | x-smwebmail / yes | E-Mail mit diesem Kennzeichen werden mittels GINA-Technologie verschlüsselt (Stichwort Lesebestätigung) |
| [emptypw] | | Die Notwendigkeit der Eingabe eines Initialpasswortes bei GINA-E-Mails wird unterdrückt (Sicherheitstechnisch bedenklich) |
| [SMS:<Mobil funknummer>] | | Mobilfunknummer zur Übertragung des Initialpasswortes einer GINA-E-Mail* |
| [noenc] | x-smplain / yes | Verschlüsseln wird unterdrückt, sofern dies als Standard im Ruleset definiert wurde |
| [sign] | x-smsign / yes | Anfordern der Signierung |
| [nosign] | x-smnosign / yes | Signieren wird unterdrückt, sofern dies als Standard im Ruleset definiert wurde |
| [lfm] | | Aktiviert das Large File Management, unabhängig der E-Mail Grösse* |
| [lfm:nocrypt] | | Der Empfänger Einer LFM Mail muss sich für das Abholen des "Large Files" nicht authentifizieren* |

**Tabelle 1**

**(*Funktionen, welche Zusatzllizenzen erfordern)**

Um den Benutzerkomfort zu steigern steht für Microsoft Outlook ein **AddIn** 104 zum kostenfreien Download Verfügung.
Soll das Ansteuern der Appliance aus IBM Notes mittels X-Header erfolgen, so kann das über eine angepasste Mailschablone realisiert werden. Für Novell Groupwise ist das Verwenden von X-Headern gegebenfalls über eine Vorlage umzusetzen.

Weitere, automatisierte Steuerungsmöglichkeiten sind zum Beispiel auch über LDAP-Abfragen möglich (siehe auch **Mail Processing** 147 **Ruleset Generator** **Custom Commands**), welche an dieser Stelle nicht näher erörtert werden.

Diese Basis Steuerungsmöglichkeiten sind bereits vordefiniert. Eine genaue Beschreibung der Konfigurationsmöglichkeiten zur Steuerung der Appliance ist unter **Mail Processing** 147 **Ruleset Generator** zu finden.

© 2015 SEPPmail AG

## 4.9 Clustern mehrer Systeme

Dieses Kapitel beschreibt die grundsätzliche Funktionsweise von Clustern sowie und zeigt die Möglichkeiten des Einbindens von SEPPmail-Appliances auf.

Die SEPPmail-Appliance verfügt über alle notwendigen Funktionen für ein eigenständiges Clustering und Loadbalancing. Natürlich ist das Einbinden in Infrastrukturen mit bereits vorhandenen externen Loadbalancern beziehungsweise Loadbalancing Verfahren ebenso möglich.

### 4.9.1 Allgemein

Ein Cluster bezeichnet einen Rechnerverbund aus mehreren vernetzten Computersystemen. Diese miteinander vernetzten Computersysteme sind zwar physisch getrennt werden aber logisch als eine Einheit betrachtet. So ist es möglich, dass ein Cluster als ein einziges logisches System angesprochen werden kann, tatsächlich aber aus mehreren physikalischen Systemen besteht.
Das Einrichten beziehungsweise das Hinzufügen von Maschinen zu einem Cluster erfolgt - wie in "Abbildung 1" dargestellt - im Menü **Cluster** (siehe auch Cluster 195).

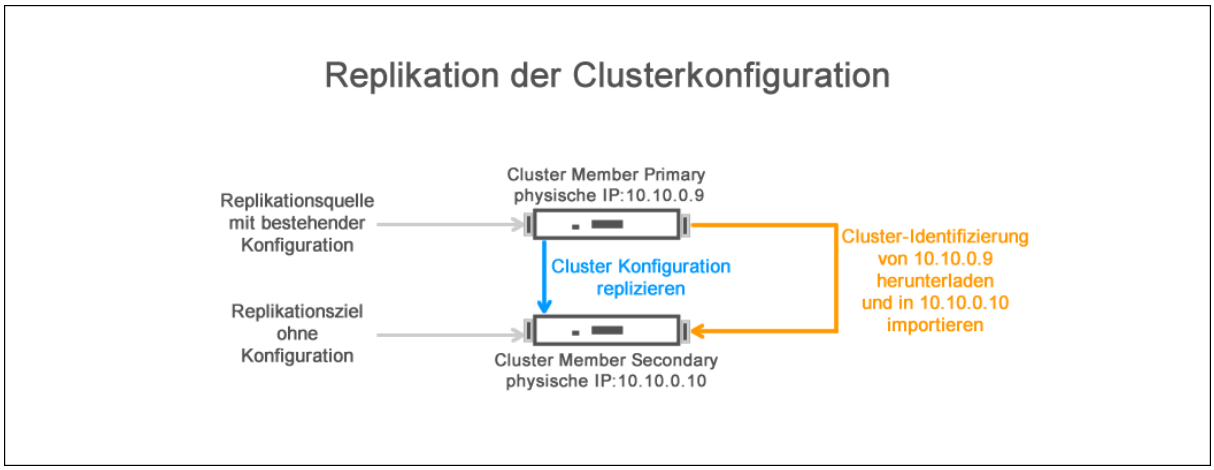



**Abbildung 1 - Einrichten eines Clusters**

Bei einem bestehenden Cluster synchronisieren alle Cluster Members ihre Konfigurationsdatenbanken ohne merklichen Zeitverlust. Das heisst alle Cluster Members sind gleichberechtigt. Konfigurationsänderungen werden somit sofort übernommen, egal an welchem Cluster Member sie vorgenommen werden ("siehe Abbildung 1.1")

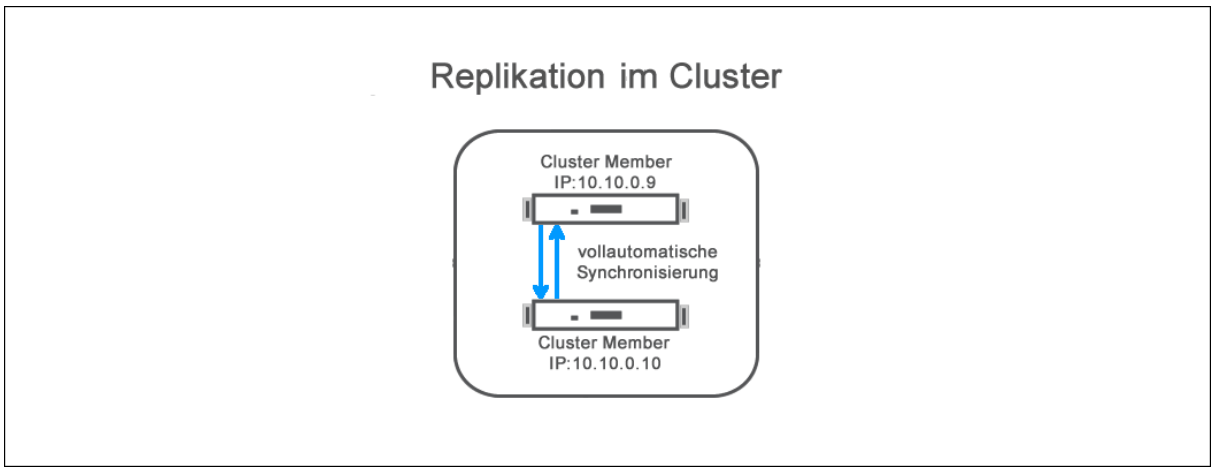



**Abbildung 1.1 - Replikation im Cluster**

© 2015 SEPPmail AG

Für das Einrichten beziehungsweise den Betrieb eines Clusters gibt es mehrere Beweggründe. Je nach Zielsetzung unterstützt die SEPPmail-Appliance verschiedene Betriebsarten, welche wie folgt unterschieden werden:

1. **Hochverfügbarkeits Cluster** 89
   Diese Art des Clusters dient dem Gewährleisten der Ausfallsicherheit

2. **Loadbalancing Cluster** 91
   Ein Loadbalancing Cluster dient der Lastverteilung auf mehrere Maschinen. Dabei können unterschiedliche Verfahren zum Einsatz kommen.

3. **Geo Cluster** 97
   Repliziert Konfigurationsdatenbanken auf geographisch voneinander getrennten Sytemen.

4. **Frontend/Backend Cluster** 98
   Bei Frontend-Backend Clustern verfügt das Frontend System über keine eigene Datenbank, sondern wird bei Bedarf vom Backend-System mit Daten gespeist. Somit kann die Frontend Maschine in einer Demilitarisierten Zone (DMZ) betrieben werden, in welcher keine Datenhaltung erlaubt ist.

5. **Secure Webmail Satellite** 99
   Trennung der GINA-Technologie vom E-Mail verarbeitenden System (Stichwort DMZ-Struktur).

6. **Unterstützen externer redundanter Systeme** 100

Dabei sind auch Kombinationen aus den verschiedenen Betriebsarten möglich.

Die zumeist benötigten virtuellen IP Adressen (IP Alias Adressen) für das Ansprechen eines Clusters als logische Einheit ist im Menü **System** (siehe auch **System** 119 **Advanced View** **IP ALIAS Addresses**) vorzunehmen.

**Hinweis:**
Bei der Dimensionierung der Anzahl und Leistungsfähigkeit der Systeme in einem Cluster ist immer darauf zu achten, dass bei Ausfall eines Systems das oder die verbleibende(n) System(e) die dadurch entstehende Mehrlast verarbeiten kann/ können.

© 2015 SEPPmail AG

### 4.9.2 Hochverfügbarkeits Cluster

Die Ausfallsicherheit des SEPPmail Systems kann durch die Bildung eines Clusters erhöht werden.

Das SEPPmail System besitzt eine integrierte Clusterfunktionalität auf Basis des CARP Protokolls (siehe auch http://de.wikipedia.org/wiki/Common_Address_Redundancy_Protocol).

Um einen Cluster zu bilden sind mindestens zwei SEPPmail-Systeme erforderlich die sich gegenseitig überwachen. Fällt ein System aus bzw. antwortet dieses nicht mehr auf Überwachungsanfragen, so übernimmt das zweite System dessen Funktion. Ist das ausgefallene System wieder verfügbar bzw. es antwortet wieder auf Überwachungsanfragen, so übernimmt es wieder seine ursprüngliche Aufgabe.

Diese Funktion kann mit bis zu neun SEPPmail-Systemen abgebildet werden, wodurch eine sehr hohe Ausfallsicherheit erreicht werden kann.

Das Hochverfügbarkeitscluster kann sowohl mit SEPPmail-Systemen auf Hardware Basis wie auch auf Basis von virtualisierten Appliances abgebildet werden. Ein Mischbetrieb beider Systeme ist ebenso möglich.

**Funktion eines Hochverfügbarkeits Clusters**

Bei diesem Verfahren werden einem Cluster eine oder mehrere virtuelle IP Adresse(n) mit verschiedenen Prioritäten zugeordnet. Jedes Cluster Member System hat unabhängig von der zugewiesenen virtuellen Cluster IP-Adresse eine jeweils eigene eindeutige IP-Adresse. Über diese eigene eindeutige IP-Adresse kann jedes Cluster Member System explizit angesprochen werden.

**Beispiel:**
In der folgenden Abbildung ist die virtuelle Cluster IP-Adresse des Clusters 10.10.0.1. Die Cluster Member Systeme haben in unserem Beispiel die IP Adressen **10.10.0.9** und **10.10.0.10**.

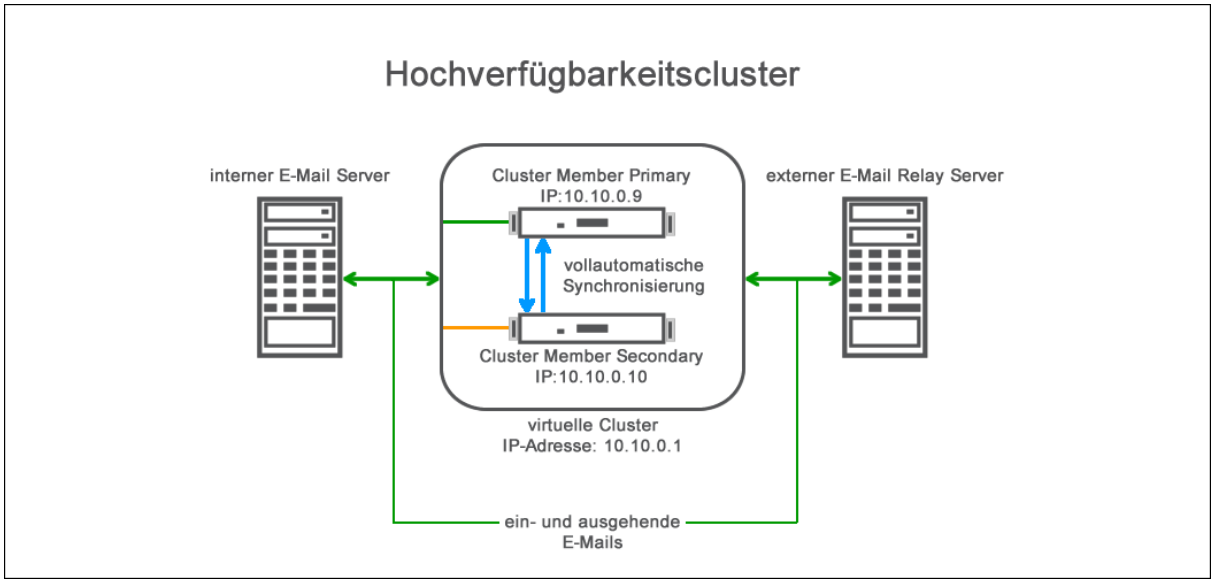



**Abbildung 2 - Schematische Darstellung eines Hochverfügbarkeitsclusters**

Das Cluster selbst wird von anderen Systemen, zum Beispiel einem internen E-Mail Server oder einem vorgelagerten E-Mail Relay Server (Gateway) über die eingerichtete(n) virtuelle(n) IP-Adresse (n) angesprochen. Im Beispiel oben ist das die IP-Adresse **10.10.0.1**.

Wird das Cluster selbst über seine Cluster IP-Adresse angesprochen, so reagiert immer das Cluster Member System mit der höchsten Priorität auf die angesprochene virtuelle Cluster IP-Adresse. Alle anderen Cluster Member Systeme mit niedrigerer Priorität reagieren nicht auf die virtuelle Cluster IP-Adresse, solange ein Cluster Member System mit einer höheren Priorität verfügbar ist.

© 2015 SEPPmail AG

Fällt das Cluster Member System mit der höchsten Priorität aus, so übernimmt automatisch ein Cluster Member System mit der nächst niedrigeren Priorität die virtuelle Cluster IP Adresse inclusive der Funktion des ausgefallenen Cluster Member Systems.

Die Prioritäten sind in der folgenden Reihenfolge geordnet:

1. Primary
2. Secondary
3. Backup

Das Einrichten der Priorität des jeweiligen Cluster Member Systems ist im Menü **System** (siehe auch System 119 Advanced View IP ALIAS Addresses Priority) vorzunehmen.

© 2015 SEPPmail AG

### 4.9.3 Loadbalancing Cluster

Ein Loadbalancing innerhalb eines Clusters kann durch mehrere Verfahren erreicht werden. Dabei bietet SEPPmail ein in die Appliance integriertes Verfahren an. Ebenso kann eine Lastverteilung auf die einzelnen Cluster Member eines SEPPmail-Clusters durch externe Loadbalancer oder Loadbalancing Verfahren erfolgen. Die gängigsten werden an dieser Stelle aufgeführt:

- Aufteilen des Ein- und Ausgehenden Verkehrs 91
  auf je ein Cluster Member System. Das Abgeben von E-Mails an den Cluster Partner tritt dabei erst bei Erreichen eines entsprechenden Lastzustandes in Kraft.
- Nutzen des DNS Round Robin Verfahrens 93
- Nutzen eines externen Loadbalancers 95

Das Failover-Verhalten des Clusters wird durch diese Konfigurationen nicht verändert.

#### 4.9.3.1 Aufteilen des Ein- und Ausgehenden Verkehrs

Das Aufteilen des ein- und ausgehenden E-Mail Datenflusses erfolgt - wie in "Abbildung 2" dargestellt - durch eine statische Konfiguration, in welcher neben den physikalischen IP-Adressen der Appliances mit zwei weiteren, virtuellen IP Adressen (IP Alias Adresses) gearbeitet wird. Dabei existieren zwei SEPPmail-Systeme die mit entgegengesetzter Priorität auf die zwei virtuellen IP-Adressen reagieren. Dadurch erhält jeweils das eine System alle eingehenden und das andere alle ausgehenden E-Mails.

**Im Detail**

Ausfallsicherheit

Jedes SEPPmail System hat eine eigene, physikalische IP-Adresse über welche nur dieses System angesprochen werden kann. Diese Adresse wird in der Regel für die individuelle Konfiguration der Appliance und für das Synchronisieren der Appliances untereinander (blaue Pfeile "Abbildung1") verwendet. in "Abbildung 2" sind dies die IP-Adressen **10.10.0.9** und **10.10.0.10**.

Zusätzlich werden zwei virtuelle IP-Adressen eingerichtet, um die beiden SEPPmail-Systeme logisch zu jeweils einer Gruppe zusammenzufassen. In "Abbildung 2" sind diese virtuellen IP-Adressen (Gruppen) farblich getrennt dargestellt.
Dabei wird die **virtuelle IP-Adresse 10.10.0.1 (grün)** vom internen E-Mail Server für das Versenden **ausgehender E-Mails** angesprochen. Da diese **virtuelle IP-Adresse** von der Maschine mit der physikalischen **IP 10.10.0.9 primär** bedient wird, fliesst der gesamte ausgehende E-Mail Verkehr im Normalbetrieb über dieses System.
Die **virtuelle IP-Adresse 10.10.0.2 (orange)** wird vom externen E-Mail Server oder auch einem vorgelagerten E-Mail Relay (zum Beispiel Firewall) für das Empfangen **eingehender E-Mails** angesprochen. Da diese **virtuelle IP-Adresse** von der Maschine mit der physikalischen **IP 10.10.0.10 primär** bedient wird, fliesst der gesamte eingehende E-Mail Verkehr im Normalbetrieb über dieses System.

In "Abbildung 2", **grün dargestellt**, ist die **virtuelle IP-Adresse 10.10.0.1** für alle ausgehenden E-Mails zuständig. Hier ist das Cluster Member System mit der IP-Adresse **10.10.0.9** als **Primary** eingerichtet und reagiert immer als erstes System, wenn die **virtuelle IP-Adresse 10.10.0.1** angesprochen wird. Das Cluster Member System mit der IP-Adresse **10.10.0.10** ist als **Secondary** eingerichtet und reagiert nur dann, wenn der Cluster Member **Primary** - also das System mit der **IP 10.10.0.9** - nicht verfügbar ist.

In "Abbildung 2", **orange dargestellt**, ist die **virtuelle IP-Adresse 10.10.0.2** für alle eingehenden E-Mails zuständig. Hier ist das Cluster Member System mit der IP-Adresse **10.10.0.10** als **Primary** eingerichtet (entgegengesetzt der vorherigen Darstellung) und reagiert somit immer als erstes System,

© 2015 SEPPmail AG

wenn die virtuelle IP-Adresse 10.10.0.2 angesprochen wird. Das Cluster Member System mit der IP-Adresse **10.10.0.9** ist als **Secondary** eingerichtet und reagiert nur dann, wenn der Cluster Member **Primary** - also das System mit der **IP 10.10.0.10** - nicht verfügbar ist.

Das heisst, fällt in diesem Konstrukt eine Maschine aus, so übernimmt die jeweils andere Maschine deren Aufgabe. Am Beispiel der "Abbildung 2" würde also bei Ausfall des Systems mit der physikalischen **IP 10.10.0.9** - welches primär den ausgehenden E-Mail Verkehr über die **virtuelle IP-Adresse 10.10.0.1** annimmt - ausfallen, so würde das **secundär** für die **virtuelle IP-Adresse 10.10.0.1** konfigurierte System - also das mir der **IP 10.10.0.10** - den ausgehenden E-Mail Verkehr zusätzlich übernehmen.

Loadbalancing

Um gegebenenfalls Lastspitzen abfangen zu können, bietet die SEPPmail-Appliance in einer solchen Umgebung weiterhin die Möglichkeit, bei erreichen eines definierten Lastzustandes am **Primary** System Last an das **Secondary** System abzugeben (siehe auch System 119 Advanced View SMTP Loadbalancing)

**Zusammenfassung**

Jedes einzelne SEPPmail System kann über zwei verschiedene virtuelle IP-Adressen angesprochen werden und reagiert mit jeweils unterschiedlichen Prioritäten einmal als **Primary** und einmal als **Secondary**. Dadurch ist der Betrieb beim Ausfall eines Cluster Member Systems weiterhin möglich. Das verbliebene Cluster Member System übernimmt dann zusätzlich die Arbeit des nicht mehr verfügbaren Systems und wird alle ein- und ausgehenden E-Mails verarbeiten.

Für die Nutzung von Enhanced Secure Webmail kann eine virtuelle Cluster IP-Adresse 10.10.0.1 angesprochen werden. In Abhängigkeit der Cluster Member Prioritäten wird im Beispiel in Abbildung 2 das Cluster Member System mit der IP-Adresse **10.10.0.9** antworten, da dies mit der Priorität **"Primary"** eingerichtet ist. Ist dieses System nicht verfügbar, so wird das Cluster Member System mit der IP-Adresse **10.10.0.10** antworten, da dies mit der Priorität **"Secondary"** eingerichtet ist.

Das Einrichten der virtuellen IP-Adressen und das Zuweisen den Prioritäten des jeweiligen Cluster Member Systems ist im Menü **System** (siehe auch System 119 Advanced View IP ALIAS Addresses) vorzunehmen.

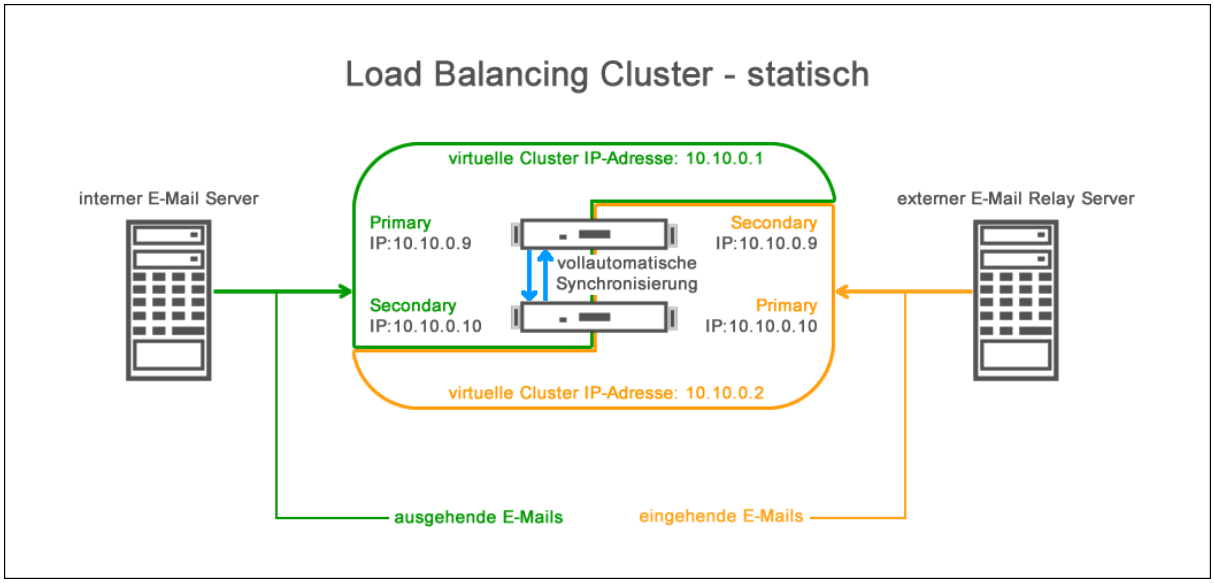



**Abbildung 2 - Schematische Darstellung der statischen Aufteilung für ein- und ausgehenden E-Mails**

© 2015 SEPPmail AG

#### 4.9.3.2 Nutzen des DNS Round Robin Verfahrens

In der Konfiguration des internen und externen E-Mail Servers wird nicht mehr eine virtuelle Cluster IP-Adresse für den E-Mail Versand angegeben sondern jeweils ein Hostname, zum Beispiel **"SEPPmail.meinefirma.ch"** der bei ein- und ausgehenden E-Mails angesprochen wird. Im DNS ist es möglich zu jedem Hostnamen mehrere IP-Adressen anzugeben. Dadurch kann eine einfache Lastverteilung erreicht werden.

Fragt nun zum Beispiel der interne E-Mail Server den für den E-Mail Versand angegebenen Hostnamen **(SEPPmail.meinefirma.ch)** des SEPPmail Clusters beim DNS Server an, so werden immer alle - diesem Hostnamen zugeordneten - IP-Adressen, also **10.10.0.1** und **10.10.0.2** zurückgeliefert, dies aber jedes Mal in unterschiedlicher Reihenfolge. Der interne E-Mail Server wird im Normalfall die erste vom DNS Server gelieferte IP-Adresse für den Versand der E-Mail verwenden.

Durch das verwenden virtueller IP-Adressen in diesem Aufbau, wird die Ausfallsicherheit gewährleistet, da in diesem Fall bei ausfall einer Maschine die verbleibende Maschine beide (virtuelle) IP-Adressen bedienen wird. "Abbildung 3" zeigt eine logische Darstellung des Szenarios.

**Im Detail**

Jedes SEPPmail System hat eine eigene, physikalische IP-Adresse über welche nur dieses System angesprochen werden kann. Diese Adresse wird in der Regel für die individuelle Konfiguration der Appliance und für das Synchronisieren der Appliances untereinander (blaue Pfeile "Abbildung 3") verwendet. In "Abbildung 3" sind dies die IP-Adressen **10.10.0.9** und **10.10.0.10**.

Zusätzlich werden zwei virtuelle IP-Adressen eingerichtet, um die beiden SEPPmail-Systeme logisch zu jeweils einer Gruppe zusammenzufassen. In "Abbildung 3" sind diese virtuellen IP-Adressen (Gruppen) farblich getrennt dargestellt.

Der interne und der externe E-Mail Server sprechen für den Versand von ein- und ausgehenden E-Mails an das SEPPmail Cluster System einen Hostnamen (SEPPmail.meinefirma.ch)statt virtueller IP-Adressen an. Wird eine Anfrage für diesen Hostnamen an den DNS-Server gestellt, so wird der Hostname in alle eingerichteten IP-Adressen aufgelöst.

Im Beispiel entsprechen die aufgelösten IP-Adressen den virtuellen Cluster IP-Adressen wie in "Abbildung 3" dargestellt.
Dabei sind die Rollen Primary und Secondary, für das Verarbeiten dieser virtuellen IP-Adressen auf den beiden Systemen entgegengesetzt konfiguriert (Stichwort Ausfallsicherheit).

Die **virtuelle IP-Adresse 10.10.0.1 (grün)** und die **virtuelle IP-Adresse 10.10.0.2 (orange)** dargestellt, werden dem Hostnamen (SEPPmail.meinefirma.ch) zugeordnet.
Wird dieser Hostname am DNS Server abgefragt, so gibt dieser bei jeder ersten Anfrage

```
SEPPmail.meinefirma.ch   1800  IN  A  10.10.0.1
SEPPmail.meinefirma.ch   1800  IN  A  10.10.0.2
```

zurück. Bei jeder zweiten Anfrage wird der DNS Server die zugeordneten IP-Adressen in umgekehrter Reihenfolge

```
SEPPmail.meinefirma.ch   1800  IN  A  10.10.0.2
SEPPmail.meinefirma.ch   1800  IN  A  10.10.0.1
```

zurückgeben. Da das Anfragende System in der Regel die jeweils zuerst gelieferte IP-Adresse verwendet entsteht so eine zahlenmässige Aufteilung der Anfragen und dadurch eine Lastverteilung.

**Zusammenfassung**

Beim Versand von ein- und ausgehenden E-Mails über das SEPPmail Cluster wird statt einer virtuellen Cluster IP-Adresse ein Hostname im jeweiligen E-Mail Server angegeben. Dieser wird dann zur

© 2015 SEPPmail AG

Laufzeit in die zugehörigen IP-Adressen aufgelöst. So können der interne und der externe E-Mail Server ein- und ausgehende E-Mails wahlweise an eine dieser aufgelösten IP-Adressen senden. Durch den Einsatz virtueller Cluster IP-Adressen reagieren die Cluster Member Systeme je nach Priorität, wodurch die Ausfallsicherheit gewährleistet wird.

Durch die DNS Round-Robin-Funktion kann für den ein- und ausgehenden E-Mail Datenfluss eine Lastverteilung erreicht werden.

Quelle: Wikipedia, http://de.wikipedia.org/wiki/Lastverteilung_per_DNS

Das Einrichten der virtuellen IP-Adressen und das Zuweisen den Prioritäten des jeweiligen Cluster Member Systems ist im Menü **System** (siehe auch System 119 **Advanced View** **IP ALIAS Addresses**) vorzunehmen.

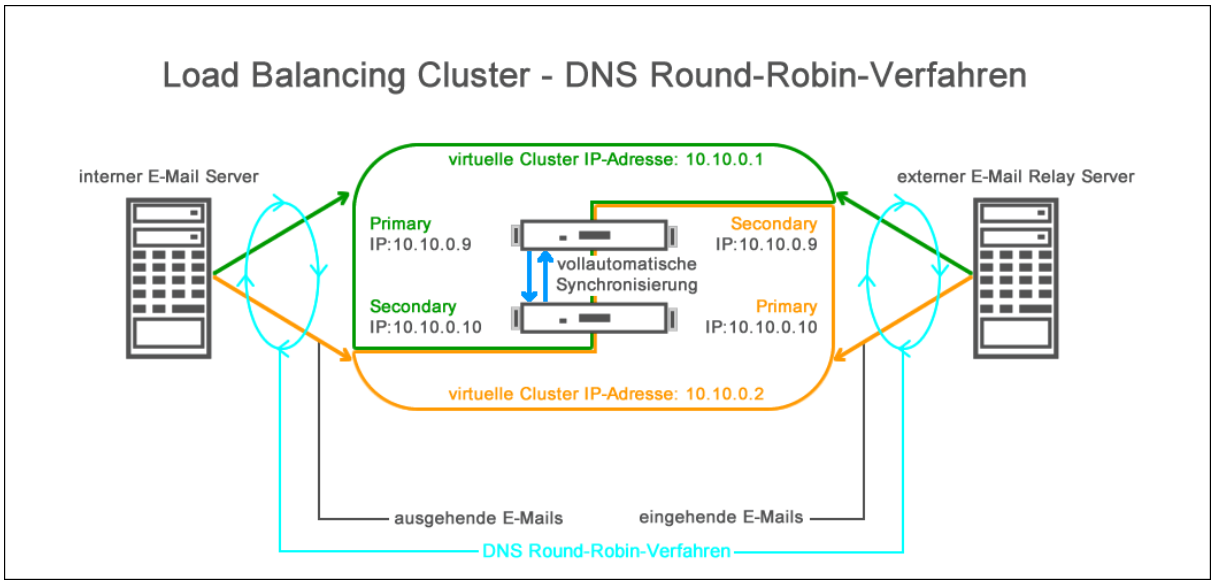



**Abbildung 3 - Schematische Darstellung der Lastverteilung durch das DNS Round-Robin-Verfahren für ein- und ausgehende E-Mails**

© 2015 SEPPmail AG

#### 4.9.3.3 Nutzen eines externen Loadbalancers

Bei Einsatz externer Loadbalancer sind diese für das gleichmässige Verteilen der Last an die SEPPmail Cluster Member Systeme verantwortlich (siehe "Abbildung 4"). Ebenso müssen diese externen Loadbalancing Systeme den Ausfall eines Cluster Member Systems erkennen und somit für die Ausfallsicherheit des Gesamtsystems sorgen.

**Im Detail**

Die Cluster-Funktionalität von SEPPmail wird in diesem Szenario lediglich für die Synchronisation der Konfiguration zwischen den Cluster Member Systemen verwendet. Das **Entscheiden**, welches System auf ein- und ausgehende E-Mails reagiert wird **durch vorgelagerte Loadbalancer** getroffen. Diese verteilen je nach Konfiguration und Lastsituation die E-Mails wahlweise an ein bestimmtes Cluster Member System. Hierbei wird jedes Cluster Member System - im Gegensatz zu den anderen Cluster Varianten - über seine eigene, physikalische IP-Adresse angesprochen. In "Abbildung 4.1" sind dies die IP-Adressen **10.10.0.9** und **10.10.0.10**.

Zu beachten ist an dieser Stelle das Realisieren des SSL Zugriffs für Enhanced Secure Webmail ( **grün** dargestellt). Kann dieser nicht wie in "Abbildung 4.1 dargestellt von einem externen Loadbalancer mit verarbeitet werden, so besteht bei Bedarf die Möglichkeit, diesen Zugriff über eine virtuelle Cluster IP-Adresse (siehe "Abbildung 4.2") - im Beispiel **10.10.0.1** - zu realisieren. In Abhängigkeit der Cluster Member Prioritäten wird im Beispiel der "Abbildung 4.2" das Cluster Member System mit der IP-Adresse 10.10.0.9 antworten, da dies mit der Priorität "**Primary**" eingerichtet ist. Ist dieses System nicht verfügbar, so wird das Cluster Member System mit der IP-Adresse 10.10.0.10 und der Priorität "**Secondary**" die Funktion übernehmen.

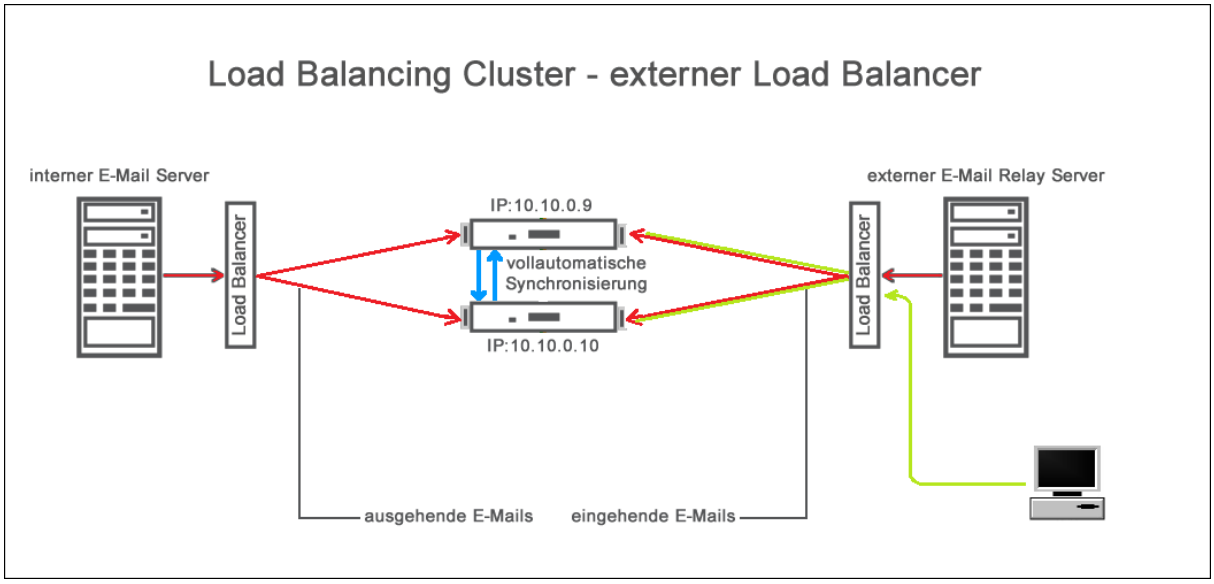



**Abbildung 4.1 - Schematische Darstellung der dynamischen Aufteilung für ein- und ausgehende E-Mails durch einen externen Loadbalancer**

© 2015 SEPPmail AG

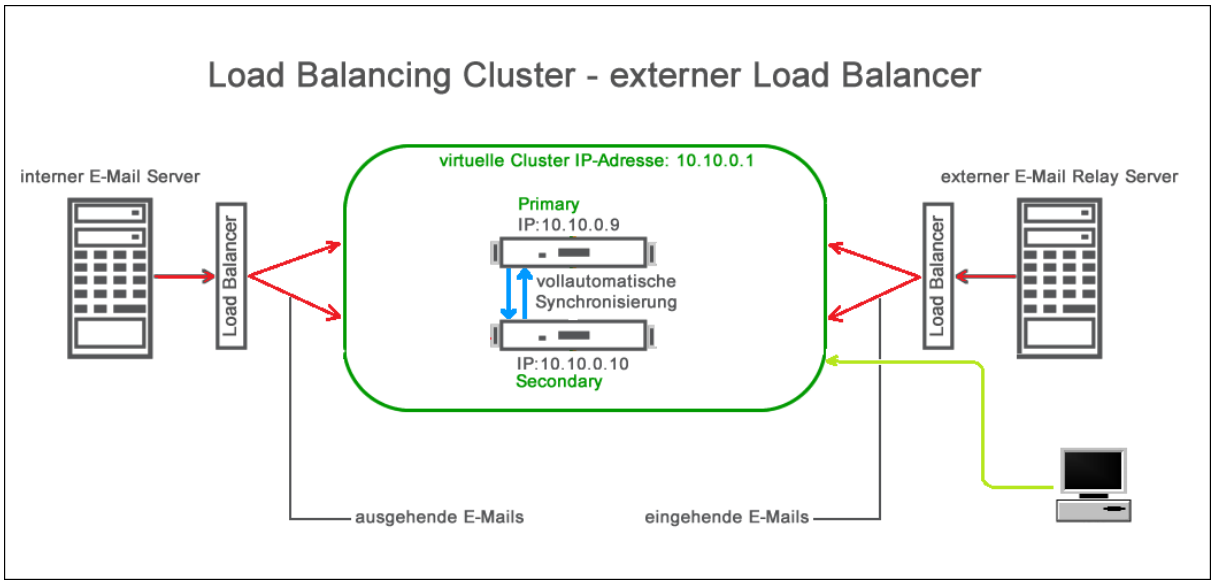



**Abbildung 4.2 - Schematische Darstellung der dynamischen Aufteilung für ein- und ausgehende E-Mails durch einen externen Loadbalancer unter Verwendung einer virtuellen IP-Adresse für Enhanced Secure Webmail**

© 2015 SEPPmail AG

### 4.9.4 Geo Cluster

Ein Geo-Cluster (auch "Multisite System" genannt) dient dem Replizieren von Konfigurationsdatenbanken zwischen geographisch voneinander getrennten SEPPmail-Systemen, zum Beispiel zwischen verschiedenen Standorten eines Unternehmens.

**Beispiel**

Ein Unternehmen ist weltweit tätig und betreibt aus diesem Grund mehrere Rechenzentren auf verschiedenen Kontinenten. Die Unternehmensstandorte selbst sind alle durch ein VPN verbunden und haben in jedem Rechenzentrum einen Zugang zum Internet. Innerhalb dieses internen Unternehmensnetzwerks besteht ein E-Mail Transportsystem, zum Beispiel auf Basis von Microsoft Exchange oder IBM Domino. Die nach extern gesendeten E-Mails können je nach intern abgebildeter Richtlinie an verschiedenen Internetzugängen des Unternehmens ins Internet versendet werden. So können beispielsweise bei Ausfall eines Internetzugangs an einem Standort die E-Mails dieses Standortes über den Internet Zugang eines Anderen Standortes versendet werden, sofern die VPN-Verbindung zwischen den Standorten von diesem Ausfall nicht betroffen ist.
In einem derartigen Konstrukt muss die notwendige kryptographische E-Mail Verarbeitung an allen Internetzugängen gleichermassen funktionieren. Um dies zu gewährleisten, müssen die Konfigurationsdatenbanken sowie das Schlüsselmaterial an allen Kryptographie-Gateways - SEPPmail-Appliances - identisch gehalten werden.

Dies wird durch die Geo-Cluster Funktion des SEPPmail-Systems realisiert, so dass stets die konsistente Konfiguration aller Systeme gewährleistet ist.

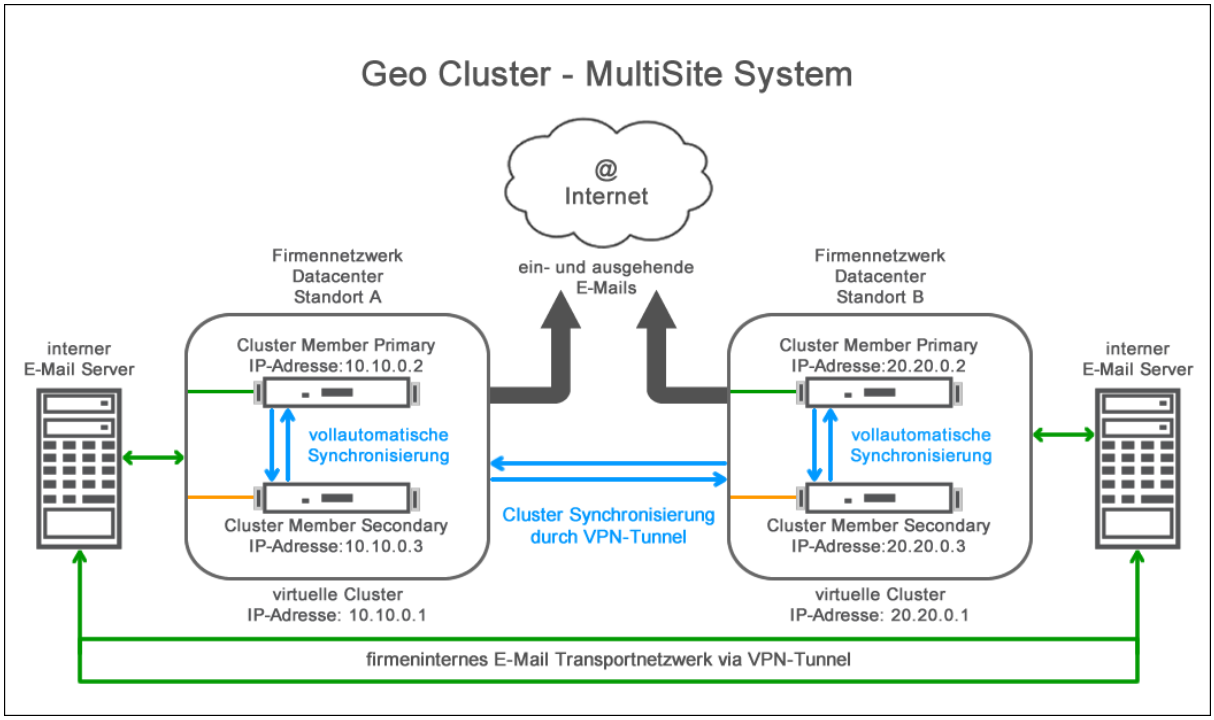



**Abbildung 5 - Schematische Darstellung einer Geo-Cluster Struktur**

© 2015 SEPPmail AG

### 4.9.5 Frontend/Backend Cluster

Ist aufgrund einer DMZ (DeMilitarisierte Zone) Struktur die Datenhaltung - insbesondere die Schlüsselverwaltung - innerhalb des Netzwerk-Standortes des E-Mail verarbeitenden Systems nicht erlaubt, so ermöglicht der  Frontend/Backend Cluster das Trennen der Datenbank vom E-Mail verarbeitenden System.

Das heisst bei dieser speziellen Form eines SEPPmail-Clusters existiert auf dem als Frontend konfigurierten System keine Konfigurationsdatenbank. Die zur Laufzeit benötigten Konfigurationsdaten werden ausschliesslich auf dem Backend System - welches die Konfigurationsdatenbank und somit auch das Schlüsselmaterial beherbergt - vorgehalten und auf Anfrage vom Frontend System auf dieses im Push-Verfahren geschoben (lila Pfeile in "Abbildung 6").
Durch Abschluss der am Frontend System angeforderte Aktion - zum Beispiel Ver- oder Entschlüsseln - werden die hierfür angeforderten Konfigurationsdaten automatisch verworfen/gelöscht.

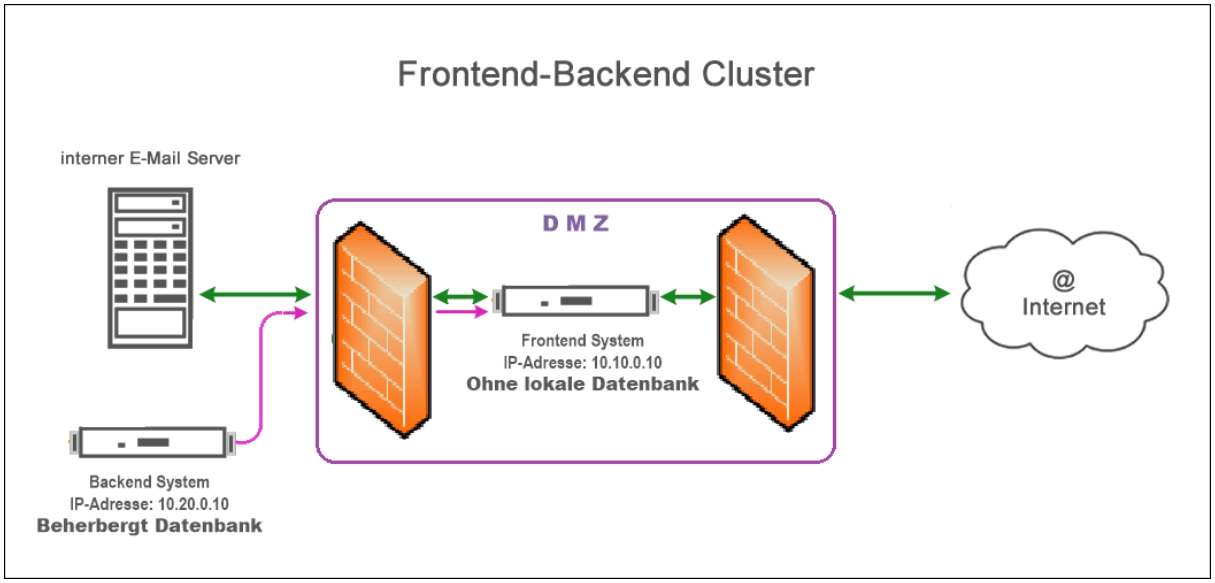



**Abbildung 6 - Schematische Darstellung einer Frontend/Backend Cluster Struktur**

© 2015 SEPPmail AG

### 4.9.6 Secure Webmail Satellite

Da E-Mail Systeme üblicherweise nur über SMTP Port 25 kommunizieren, ist unter Umständen aufgrund einer vorhandenen DMZ (DeMilitarisierte Zone) Struktur die für die GINA-Technologie benötigte Kommunikation über SSL Port 443 nicht möglich. Um dennoch die GINA-Technologie Nutzen zu können, ohne die Sicherheits-Infrastruktur aufweichen zu müssen, ist ein Abspalten dieser Technologie über das GINA Satelliten System und somit das Platzieren ausserhalb der DMZ möglich.

Die Kommunikation zwischen dem Basis System und dem Satelliten System erfolgt dabei via SMTP Port 25 (lila Pfeil in "Abbildung 7"). Zum Internet hin wird das GINA-Web Interface - meist getrennt durch eine Web Application Firewall (WAF) - über SSL Port 443 bereit gestellt.

Das Einrichten dieser speziellen Funktion erfolgt im Menü **Mail Processing** (siehe auch **Mail Processing** 147 **Ruleset Generator** **Advanced Settings**).

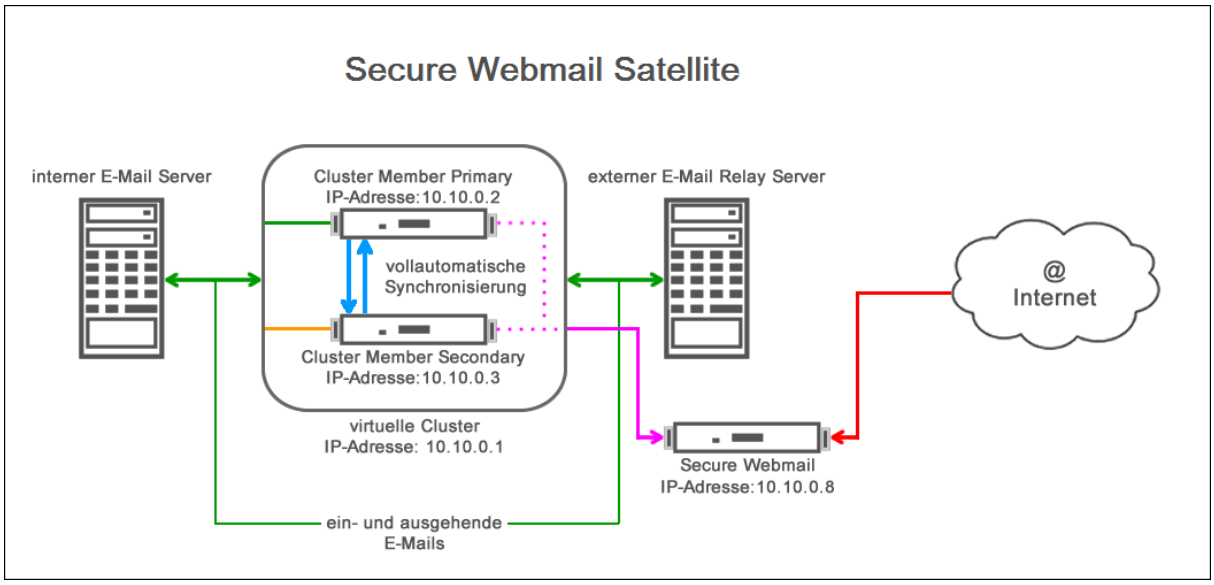



**Abbildung 7 - Schematische Darstellung einer Secure Webmail Satellite Struktur**

© 2015 SEPPmail AG

### 4.9.7 Unterstützen externer redundanter Systeme

**Einsatz mit redundanten internen und externen MTAs (Mail Transport Agent)**

In der SEPPmail Konfiguration kann sowohl als externer MTA (E-Mail Relay) (siehe Mail System 129 Outgoing Server **Server name**) wie auch pro interner E-Mail Domäne (E-Mail Server) (siehe Add/ Edit Managed Domain 136 Settings **Forwarding Server IP or MX name**) jeweils nur ein Host angegeben werden. Sollen mehrere Systeme angesprochen werden können, so muss dies über DNS MX-Einträge geschehen.

Steht lokal kein DNS-Server zur Verfügung, welcher MX-Einträge für die anzubindenden Server bereit stellt, so können hierfür im Menü System lokale (pseudo) Einträge definiert werden (siehe auch System 119 Advanced View DNS **local zone**) und verwendet werden.

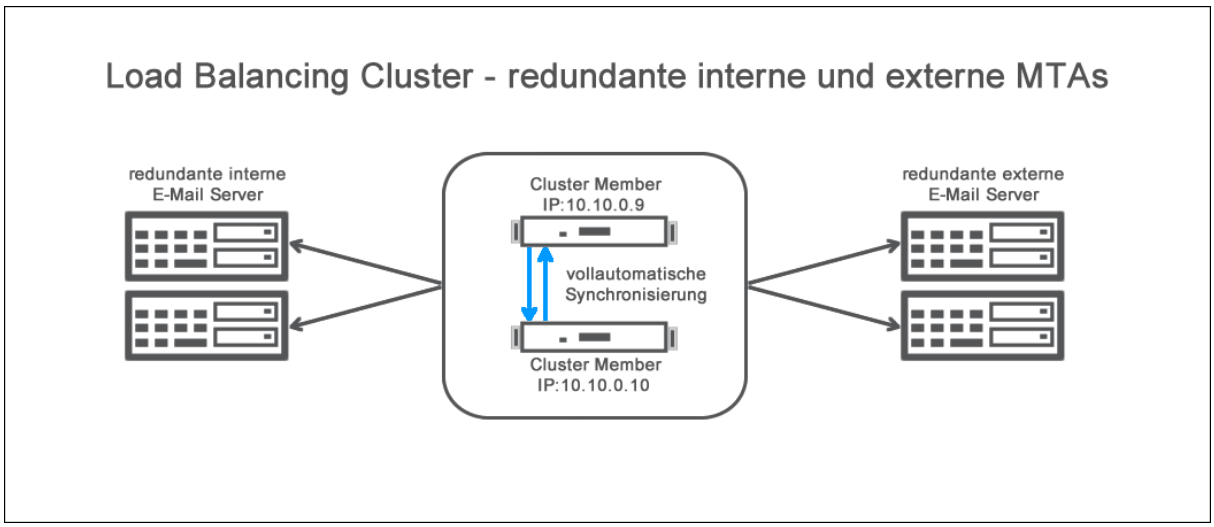



**Abbildung 8 - Schematische Darstellung für den Einsatz von redundanten internen und externen MTAs**

© 2015 SEPPmail AG

## 4.10 Einrichten zusätzlicher Features

Die SEPPmail-Appliance bietet neben der Hauptfunktion des kryptographischen Behandelns von E-Mails zusätzliche Features an, um

- die Sicherheit zu erhöhen
  - ➢ Protection Pack (VSPP) 101
  - ➢ Internal Mail Encryption (IME) 101
- den Verwaltungsaufwand zu minimieren
  - ➢ Self Service Password Management (SSPM) 102
- den Funktionsumfang zu erweitern
  - ➢ Large File Management (LFM) 102

Diese optionalen Features müssen separat lizensiert werden.

### 4.10.1 Protection Pack (VSPP)

Das Protection Pack (VSPP) bietet zusätzlichen Schutz vor Spam E-Mails und Viren.
Die für das Einrichten erforderlichen Einstellungen sind in den Sektionen **Antispam**, **Blacklists** und **Manual Blacklisting / Whitelisting** des Menüs **Mail System** (siehe Mail System 129) sowie im Menü **Mail Processing** (siehe Mail Processing 147) unter der Sektion **Ruleset Generator** im Punkt **Protection Pack (Anti-SPam / Anti-Virus)** zu finden.

### 4.10.2 Internal Mail Encryption (IME)

Die Internal Mail Encryption dient dem Verschlüsseln von E-Mails innerhalb des eigenen Unternehmens (E-Mail Domänen).
Diese Funktion wird in drei verschiedenen Ausprägungen angeboten.

Die erste Variante wird dabei über das Microsoft Outlook AddIn 104 realisiert.
Dabei muss gegebenenfalls die Schaltfläche "intern verschlüsseln" über die entsprechenden AddIn Einstellungen (siehe Registry 110 Tabelle 1) angezeigt werden. Der Absender aktiviert dann im Ribbon von Microsoft Outlook den vom AddIn bereit gestellten Schalter "intern verschlüsseln" vor Versand der der E-Mail. Bei dieser Methode wird die E-Mail zwar unverschlüsselt bis zur SEPPmail-Appliance übertragen, jedoch GINA verschlüsselt dem Empfänger zugestellt.

Für Variante zwei kommt ausschliesslich die GINA-Technologie zum Einsatz.
Das heisst der Absender einer intern zu verschlüsselnden E-Mail meldet sich bereits für den Versand dieser vertraulichen E-Mail am GINA-Web-Portal an.
Damit sich der interne Benutzer als GINA-Benutzer registrieren kann, ist das Aktivieren der Optionen
Allow account self-registration in GINA portal without initial mail
Allow GINA users to write new mails (not reply)
aus dem Untermenü Edit GINA Setting 165 - welches über **Mail Processing** **GINA Domains** **Edit** zu erreichen ist - in der Sektion **Extended Settings** notwendig.
Sollten diese Optionen für den Zugriff von extern nicht gewünscht sein, so muss gegebenenfalls für den Zugriff von intern ein eigenes GINA-Interface Create new GINA Domain 164 (siehe **Mail Processing** **GINA Domains** **Create new GINA domain**) eingerichtet werden.

Die dritte und letzte Möglichkeit erfordert das Verteilen von Schlüsselmaterial auf den Client.
So werden E-Mails intern direkt am E-Mail Client mit den ihm zur Verfügung stehenden (meist self signed) S/MIME Schlüsseln verschlüsselt. Enthält eine E-Mail einen externen Empfänger, so wird an

© 2015 SEPPmail AG

der SEPPmail-Appliance nach dem Prinzip "best effort" umverschlüsselt.

An der SEPPmail-Appliance muss für dieses Verfahren die Option
Enable internal encryption with user keys (also enables ldap server on ports 388, 387 and 635. User keys must be installed on appliance for proper function)
aus **Mail Processing** **Ruleset Generator** **Advanced Options** (siehe **Mail Processing** 147) aktiviert werden.

### 4.10.3 Self Service Password Management (SSPM)

Das Self Service Passwort Management erlaubt es GINA-Benutzern selbständig Ihr Passwort zurückzusetzen, wenn dieses verloren ging. Ein Eingreifen des Administrators ist somit nicht notwendig.
Für das Konfigurieren des eigenständigen Zurücksetzens stehen Untermenü **Edit GINA Setting** 165 - welches über **Mail Processing** **GINA Domains** **Edit** zu erreichen ist - in der Sektion **Security** die Möglichkeiten zur Rücksetzung

- über eine Bestätigungs E-Mail (**Reset by Email verification**)
- per SMS (**Reset by SMS**)
- über eine Auswahl durch den Benutzer (**Let user choose between hotline and SMS**)

bereit.

Wird die Möglichkeit des Zurücksetzens per SMS angeboten, so ist über das Menü **Mail Processing** (siehe **Mail Processing** 147) in der Sektion **GINA password via SMS** die Konfiguration des SMS Versandes vorzunehmen.

### 4.10.4 Large File Management (LFM)

Das Large File Management ermöglicht mittels GINA-Technologie die Übertragung grosser Dateien, über das übliche E-Mail Limit hinaus.
Diese zusätzliche Funktion wird im Untermenü **Edit GINA Setting** 165 - welches über **Mail Processing** **GINA Domains** **Edit** zu erreichen ist - in der Sektion **Large File Management** aktiviert und konfiguriert.

© 2015 SEPPmail AG

# 5 Administrative Aufgaben

Administrative Aufgaben wurden durch das effektive Design der SEPPmail-Appliance auf ein Minimum reduziert. Sollten dennoch Aufgaben anfallen, so werden die Mitglieder der Gruppen **admin** und **statisticsadmin** (siehe Groups 213) darüber benachrichtigt. Weiterhin werden Benachrichtigungen über Probleme des Systems per Watchdog Meldung an die **Postmaster address** (siehe Mail Processing 147 SMTP settings) gesendet.

Je nach Konfiguration des Systems lassen sich so die administrativen Aufgaben auf folgende Tätigkeiten beschränken:

- Eingreifen bei Problemen (Watchdog Meldung)
- Aktualisieren der Appliance (siehe Administration 190 Update)
- Erneuern des SSL Zertifikats bei Ablauf (siehe SSL 179)
- Einstufen der Vertrauesnwürdigkeit von X.509 Root Certificates 218

Sollte die Anlage von Benutzern (siehe Mail Processing 147 Ruleset generator **User creation**) sowie der Bezug von Zertifikaten (siehe Mail Processing 147 Ruleset generator **Key Generation**) nicht automatisiert sein, so fallen hierfür natürlich weitere Aufgaben an.

© 2015 SEPPmail AG

# 6 Microsoft Outlook AddIn

## 6.1 Einleitung

Das SEPPmail-AddIn für Microsoft Outlook kann auf PC-Systemen mit Microsoft Outlook installiert werden. Das Installieren kann sowohl interaktiv, als auch im Silent-Mode erfolgen. Je nach gewählter Installation stehen unterschiedliche Einstellungen (Parameter) zur Verfügung, um die Funktionalität des AddIns zu beeinflussen.

Das AddIn stellt im jedem Outlook Fenster zum Verfassen einer E-Mail (Neu, Weiterleiten, Antworten) Schaltflächen für das Steuern der kryptographischen Aktionen der SEPPmail-Appliance zur Verfügung. Abhängig von den bei der Installation gewählten Einstellungen erscheinen unterschiedlich viele Schaltflächen, mit unterschiedlichen Standard-Einstellungen (gedrückt / nicht gedrückt).

Die Zustände der Schaltflächen beim späteren Versenden einer E-Mail werden entweder

- als Steuer-Informationen in x-header geschrieben.
- optional bei Verwendung des "Subject-Mode" als Schlüsselwort in die Betreffzeile der E-Mail integriert.
  Da es E-Mail Server gibt, welche x-header abschneiden, bietet der "Subject-Mode hierfür eine Alternative.
  Die durch das AddIn im "Subject-Mode" hinzugefügten Schlüsselworte sind auch im "Gesendet" Ordner des Absenders zu sehen. Das versetzt diesen in die Lage, auch später nachzuvollziehen, ob er eine E-Mail kryptographisch behandelt oder unbehandelt versendet hat.

Das zentrale SEPPmail-System ist bei Eingang der E-Mail in der Lage beide Informationen auszuwerten.

Weiterhin steht eine (optionale) Schaltfläche für den Aufruf einer Hilfe-Seite im Standard-Webbrowser zur Verfügung.
Ebenso kann bei Bedarf eine Warnung beim Versenden von unverschlüsselten und unsignierten E-Mails ausgegeben werden.

Die Anwendung ist mehrsprachig und passt sich der jeweiligen Sprache der Microsoft Outlook-Oberfläche an. Ist diese nicht verfügbar, wird Englisch als Standardsprache für das AddIn verwendet. Derzeit sind die Sprachen

- Deutsch
- Englisch
- Französisch
- Italienisch

verfügbar.

Im Folgenden werden technische Details zu den System-Anforderungen, zur Installation und zu den Abläufen in der Registry beschrieben.

## 6.2 Download

Das SEPPmail-Add-In für Microsoft Outlook können Sie auf der folgenden Webseite in der jeweils aktuellen Version herunterladen:

http://dl.seppmail.ch

© 2015 SEPPmail AG

## 6.3 Systemanforderungen

Das SEPPmail-Add-In für Microsoft Outlook kann unter verschiedenen Betriebssystemen und Microsoft Outlook Versionen installiert werden:

**Microsoft Windows Betriebssysteme**

- Windows Vista
- Windows 7 (32/64 bit)
- Windows 8 (32/64 bit)
- Windows Terminal Server

**Microsoft Outlook Versionen**

- Outlook 2003
- Outlook 2007
- Outlook 2010 (32/64 bit)
- Outlook 2013 (32/64 bit)

**.NET Framework**

Das .NET Framework muss in der Version 4.0 Client Profile oder neuer vorhanden sein. Fehlt dieses, versucht die Installationsroutine diese Komponente automatisch aus dem Internet zu beziehen und zu installieren.

## 6.4 Installation

Die Installation besteht aus zwei Dateien:

- Setup.exe
  ist erforderlich um auf Windows Vista, Windows 7 und Windows 8, bei eingeschaltetem UAC ( User Account Control = Benutzerkontensteuerung), per Rechtsklick „Als Administrator“ auswählen zu können.
  Prüft vor dem Ausführen der .msi-Datei ob die Voraussetzungen für die Installation (zum Beispiel NET Framework) vorhanden sind.

- SEPPmailOutlookAddInSetup.msi
  führt die eigentliche Installation durch und kann auch direkt gestartet werden, wenn entsprechende Rechte vorhanden sind (zum Beispiel inaktives UAC und Admin-Rechte) beziehungsweise am Terminalserver bereits in den Install-Mode gewechselt wurde.

© 2015 SEPPmail AG

### 6.4.1 Interaktive Installation

Beispiel:

1. Rechtsklick auf setup.exe und „Als Administrator ausführen“ bzw. „Run as administrator“ auswählen.

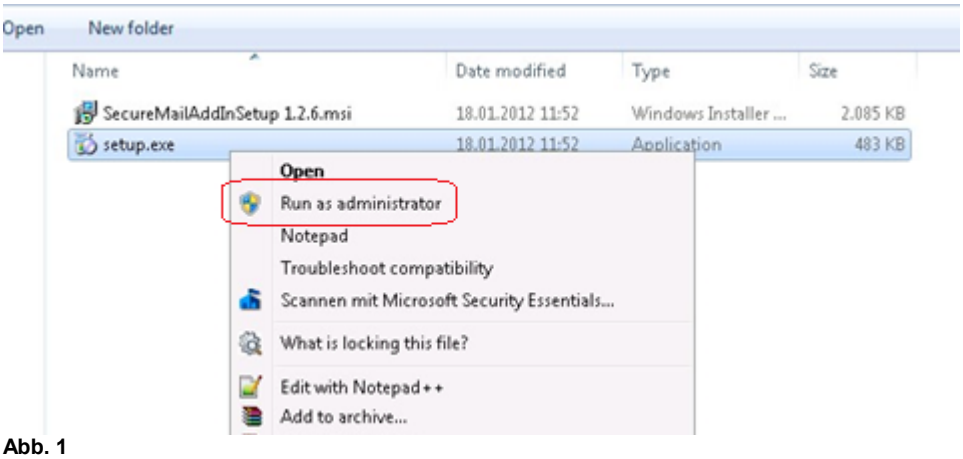



**Abb. 1**

2. Die Sicherheitsabfrage von Windows mit „Ja“ beantworten, um die Installation zu starten.

3. Im folgenden erscheinen die folgenden Bildschirme auf denen der Benutzer Wahlmöglichkeiten
   a. zu den später angezeigten Buttons

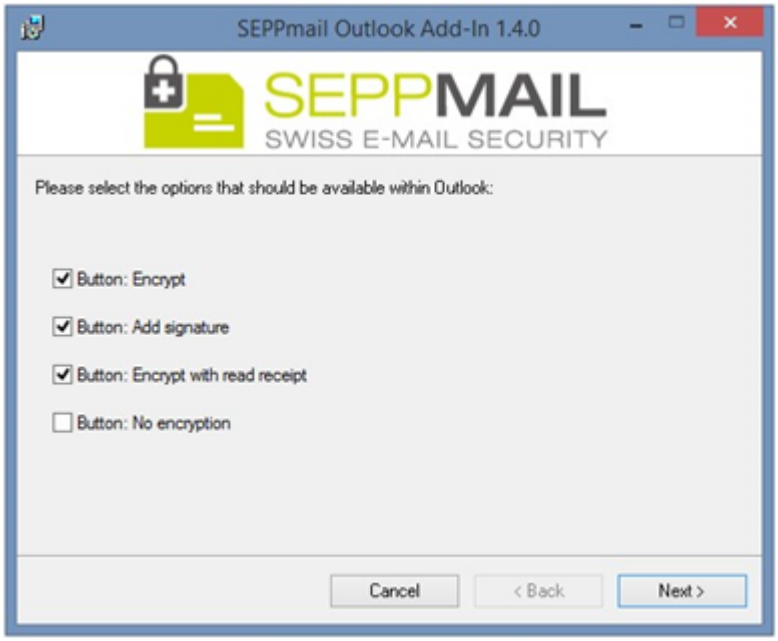



**Abb. 2**

   b. zu den Standard Button-Zuständen bei Öffnen eines E-Mail Fensters

© 2015 SEPPmail AG

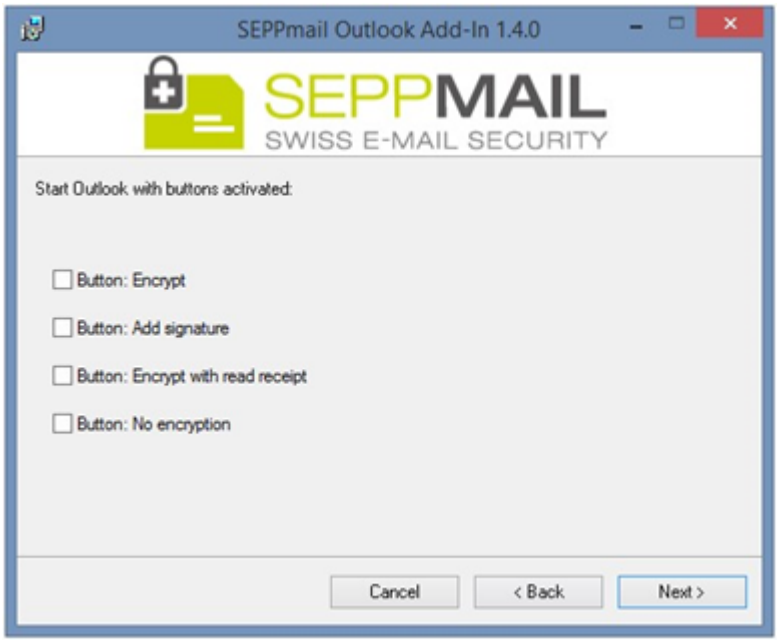



**Abb. 3**

c. zum Ein/Ausschalten einer Warnung beim Versand von unverschlüsselten und unsignierten E-Mails

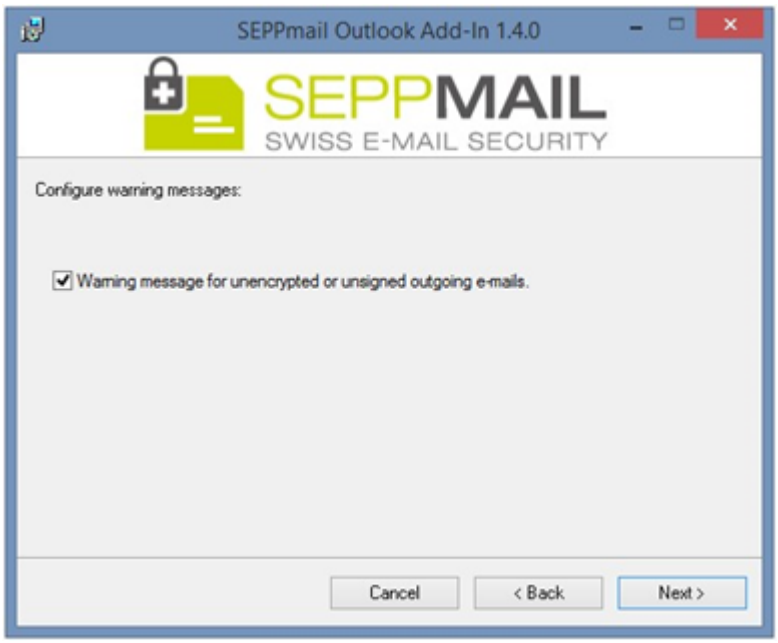



**Abb. 4**

© 2015 SEPPmail AG

### 6.4.2 Silent Installation

Alternativ kann die Installation über die Kommandozeile mit diversen Parametern gestartet werden.

**Hinweis:**
Die Kommandozeile muss als Administrator gestartet werden!

**Beispiel**

```
msiexec /q /i "SEPPmailOutlookAddInSetup.msi" SMWarning=false
SMEncrypt=true SMSign=true SMWebmail=true SMHelp=true
SMEncryptSelected=false MSignSelected=false SMWebmailSelected=false /
li .\log.txt
```

**Msiexec-Parameter:**

| Parameter | Beschreibung |
|---|---|
| /q | Installation ohne User Interface |
| /i | Installation eines MSI Paketes |
| /li .\log.txt | log.txt mit Basis Informationen im aktuellen Verzeichnis erzeugen |

**MSI-Parameter** von SEPPmailOutlookAddInSetup.msi

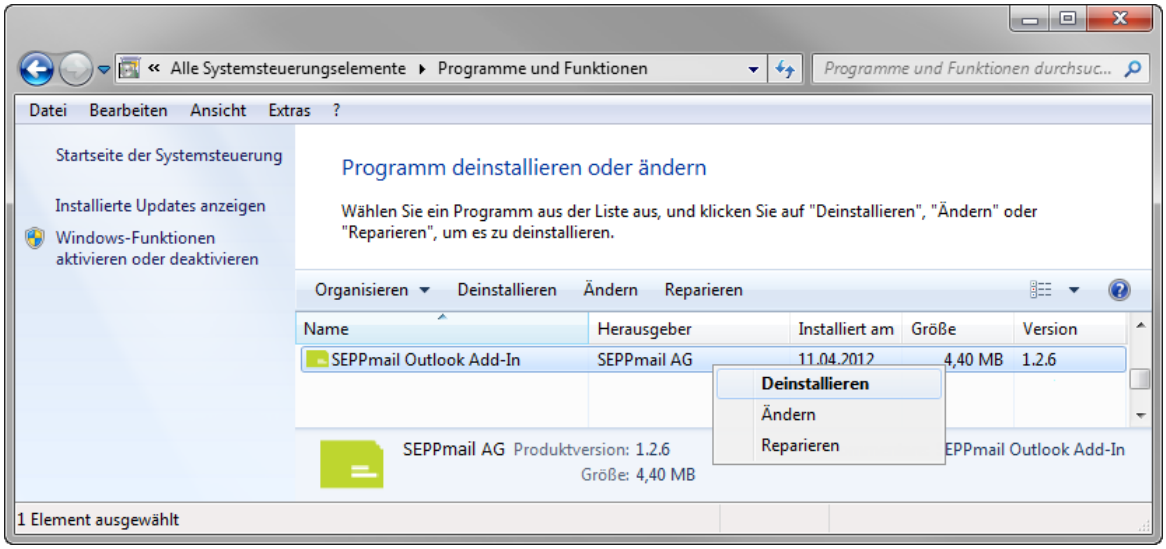
| Parameter | Standard | Beschreibung |
|---|---|---|
| SMWarning | False | Warnung falls die Schaltfläche verschlüsseln nicht ausgewählt wurde ein-/ausschalten |
| SMEncrypt | True | Schaltfläche „Verschlüsseln“ ein-/ausblenden |
| SMSign | True | Schaltfläche „Signieren” ein-/ausblenden |
| SMWebmail | True | Schaltfläche „Verschlüsseln mit Lesebestätigung” ein-/ausblenden |
| SMNoEncryption | False | Schaltfläche „Unverschlüsselt” ein-/ausblenden |
| SMHelp | False | Schaltfläche „Hilfe” ein-/ausblenden |
| SMEncryptSelected | False | Schaltfläche „Verschlüsseln” im Standard aktiv/inaktiv setzen |
| SMSignSelected | False | Schaltfläche „Signieren” im Standard aktiv/inaktiv setzen |
| SMWebmailSelected | False | Schaltfläche „Verschlüsseln mit Lesebestätigung” im Standard aktiv/inaktiv setzen |
| SMNoEncryptionSelected | False | Schaltfläche „Unverschlüsselt” im Standard aktiv/inaktiv setzen |
| Tooltips | False | Tooltips für Buttons ein-/ausschalten |
| LMonly | False | Registry-Werte nur in „HKLM“, nicht in „HCU“ speichern |

© 2015 SEPPmail AG

### 6.4.3 Deinstallation

Die Deinstallation des SEPPmail-Add-In für Microsoft Outlook erfolgt interaktiv über die **Systemsteuerung** im Menü **Programme und Funktionen**.

**Interaktiv am Beispiel Windows 7/8**
Rechtsklick auf den Eintrag **SEPPmail Outlook Add-In -> Deinstallieren**.




**Deinstallation - Outlook Add-In**

Weiterhin ist die Deinstallation auch Silent per MSI über den Befehl

MsiExec.exe /x {A5B1FA06-7E16-4645-AFC1-0A7CDAFA77E3} /qn

oder über das AddIn Setup

setup /s /v" /x {A5B1FA06-7E16-4645-AFC1-0A7CDAFA77E3} /qn"

möglich.

Dabei ist zu beachten, dass diese Befehle mit Administrator-Rechten ausgeführt werden müssen.

© 2015 SEPPmail AG

## 6.5 Registry

Das AddIn macht im Standard sowohl maschinenbezogene Eintragungen in den Registry Hive HKEY_LOCAL_MACHINE (HKLM) wie auch in die benutzerbezogenen Hives HKEY_CURRENT_USER (HCU).
Um zum Beispiel unternehmensweit Standard Vorgaben der Schaltflächen Einstellungen zu erzwingen, lässt sich das Speichern Benutzer bezogener Einstellungen (HCU) optional abschalten. Die Schaltflächen Einstellungen werden bei neuen Benutzern aus den Maschineneinstellungen (HKLM) in die Benutzereinstellungen (HCU) übernommen. Ebenso werden Änderungen der Maschineneinstellungen bei bestehenden Benutzern übernommen.

Folgend werden die Registry-Werte für das AddIn im Bereich

**HKEY_CURRENT_USER\Software\SEPPmail\OutlookAddIn**

bei **32 bit** Maschinen beziehungsweise

**HKEY_CURRENT_USER\Software\Wow6432Node\SEPPmail\OutlookAddIn**

bei **64 bit** Maschinen und Ihre jeweilige Funktion beschrieben:

| Schaltfläche | Registry | | | Beschreibung |
|---|---|---|---|---|
| | Name | Typ REG_ | Data | |
| verschlüsseln | SMEncrypt | DWORD | 0/1 | blendet die Schaltfläche aus bzw. ein |
| | SMEncrypt Selected | DWORD | 0/1 | setzt die Schaltfläche im Standard auf inaktiv/aktiv |
| | s-smenc | SZ | [confidential] | subject-mod Schlüsselwort |
| verschlüsseln mit Lesebestätigung | SMWebmail | DWORD | 0/1 | blendet die Schaltfläche aus bzw. ein |
| | SMWebmail Selected | DWORD | 0/1 | setzt die Schaltfläche im Standard auf inaktiv/aktiv |
| | s-smwebmail | SZ | [priv] | subject-mod Schlüsselwort |
| intern verschlüsseln | Internal Encryption | DWORD | 0/1 | blendet die Schaltfläche aus bzw. ein |
| | Internal Recipient | DWORD | ime@imepseudo domain.local | gibt die Pseudo Empfängeradresse für IME an |
| unverschlüsselt | SMNoEncryption | DWORD | 0/1 | blendet die Schaltfläche aus bzw. ein |
| | SMNoEncryption Selected | DWORD | 0/1 | setzt die Schaltfläche im Standard auf inaktiv/aktiv |
| | s-smplain | SZ | [plain] | subject-mod Schlüsselwort |
| signieren | SMSign | DWORD | 0/1 | blendet die Schaltfläche aus bzw. ein |
| | SMSign Selected | DWORD | 0/1 | setzt die Schaltfläche im Standard auf inaktiv/aktiv |
| | s-smsign | SZ | [sign] | subject-mod Schlüsselwort |
| Hilfe | SMHelp | DWORD | 0/1 | blendet die Schaltfläche aus bzw. ein |
| | subject-mod | DWORD | 0/1 | durch Aktivieren des subject-mod werden Betreffzeilen Schlüsselworte statt x-header zur Steuerung der Appliance verwendet. |
| | LMOnly | DWORD | 0/1 | das Aktivieren von LMOnly deaktiviert das be- nutzerbezogene |

© 2015 SEPPmail AG

| | | | | |
|---|---|---|---|---|
| | | | | Speichern von Einstellungen in HCU |
| | Tooltips | DWORD | 0/1 | de- bzw. aktiviert die Tooltips für die Schaltflächen |
| | UsageTimeStamp | SZ | 2014,4,8,16,51,27 | Zeitstempel für den Vergleich HKLM/HCU |
| | Web Site | SZ | http://www.seppmail.ch | Webseite welche bei Anklicken der Hilfe Schaltfläche aufgerufen werden soll |

**Tabelle 1**

Davon werden folgende Werte gegebenenfalls in den Bereich

**HKEY_CURRENT_USER\Software\SEPPmail\OutlookAddIn**

übernommen:

| Schaltfläche | Registry | | |
|---|---|---|---|
| | Name | Typ REG_ | Data |
| verschlüsseln | SMEncrypt | DWORD | 0/1 |
| | SMEncryptSelected | DWORD | 0/1 |
| verschlüsseln mit Lesebestätigung | SMWebmail | DWORD | 0/1 |
| | SMWebmailSelected | DWORD | 0/1 |
| intern verschlüsseln | InternalEncryption | DWORD | 0/1 |
| | InternalRecipient | DWORD | ime@imepseudodomain.local |
| unverschlüsselt | SMNoEncryption | DWORD | 0/1 |
| | SMNoEncryptionSelected | DWORD | 0/1 |
| signieren | SMSign | DWORD | 0/1 |
| | SMSignSelected | DWORD | 0/1 |
| Hilfe | SMHelp | DWORD | 0/1 |
| | UsageTimeStamp | SZ | 2014,4,8,16,51,27 |

**Tabelle 2**

Werden durch Aktivieren des **subject-mod** statt der x-header Betreffzeilen Schlüsselworte verwendet, so ist darauf zu achten, dass die Schlüsselworte der in der Appliance im Punkt **Mail Processing Ruleset generator** konfigurierten gleichen.

| x-header | Registry | |
|---|---|---|
| | Name | Schlüsselwort (Standard) |
| x-smenc | s-smenc | [confidential] |
| x-smsign | s-smsign | [sign] |
| x-smwebmail | s-smwebmail | [priv] |
| x-smplain | s-smplain | [plain] |

**Tabelle 3**

© 2015 SEPPmail AG

## 6.6 AddIn Verwaltung

Für das zentrale Verwalten der AddIn Einstellungen in Microsoft Netzwerken, bieten wir zusätzlich ein ADM-Template an. Somit können die Einstellungen bequem per  per Group Policies (GPO) ausgebraucht werden.

Die Vorlage steht ebenfalls zum **Download** 104 zur Verfügung.

© 2015 SEPPmail AG

# 7 Referenz der Menüpunkte

## 7.1 Übersicht der Menüpunkte

Die Konfigurationsoberfläche der SEPPmail-Appliance ist in die, in der folgenden Tabelle kurz beschriebenen Menüs aufgeteilt. Die Gliederung dieses Teils des Handbuchs folgt dieser Tabelle.

| Menü | Beschreibung |
|---|---|
| **Login/Logout** | Anmeldung an der Konfigurationsoberfäche, ändern des persönlichen Kennworts für die Konfigurationsoberfläche |
| **Home** | Anzeige administrativer Daten wie zum Beispiel Systemstatus, System- und Benutzerlizenz, aktuelle Softwareversion, statistische Daten zur Systemauslastung |
| **System** | Durchführen grundlegender Netzwerkeinstellungen wie zum Beispiel IP-Adresse, Host- und Domainname, Routing, System Datum- und Uhrzeit |
| **Mail System** | Einrichtung des SEPPmail E-Mail-Systems, E-Mail Domänen und E-Mail-Routing, E-Mail-Relay-Server, Access Control, TLS, AntiSPAM, Blacklists/ Whitelists |
| **Mail Processing** | Regeln zur Verarbeitung von E-Mails, Verwaltung von GINA-Domänen, SMS-Kennwortversand, Disclaimer, E-Mail-Templates, Virenscanner und SPAM-Protection-Regeln und Schwellwerte, Regelwerk für E-Mail-Signierung, Ver- und Entschlüsselung verwalten/anzeigen/laden |
| **SSL** | SSL-Device-Zertifikat für den SEPPmail Secure Webmail Webserver einrichten und sichern |
| **CA** | Eigene Zertifizierungsstelle (CA) einrichten, Connector zur SwissSign CA (MPKI) einrichten, CA-Zertifikat anfordern und sichern, eventuell Sub-CA oder Registrierungsstelle (RA) einrichten. |
| **Administration** | SEPPmail registrieren, Software-Updates installieren, Datensicherung erstellen und zurücksichern, SEPPmail neu starten oder herunterfahren, SEPPmail auf Werkseinstellungen zurücksetzen, bestehende Benutzer oder Schlüssel importieren, ausgehende Supportverbindung aktivieren |
| **Cluster** | Cluster-Verbund mit mehreren SEPPmail-Systemen einrichten |
| **Logs** | E-Mail-Logdateien einsehen und verwalten |
| **Statistics** | Grafische Anzeige des verarbeiteten E-Mail-Verkehrs und der Systemauslastung |
| **Users** | SEPPmail-Benutzerkonten erstellen und verwalten |
| **Groups** | SEPPmail-Gruppen erstellen und verwalten |
| **GINA accounts** | Verwalten von automatisch erzeugten GINA--Konten. GINA bezeichnet die frühere Secure-Webmail-Schnittstelle. |
| **openPGP public keys** | Öffentliche openPGP-Schlüssel von Kommunikationspartnern importieren und verwalten |

© 2015 SEPPmail AG

| | |
|---|---|
| **X.509 Certificates** | Öffentliche S/MIME X.509-Zertifikate von Kommunikationspartnern importieren und verwalten |
| **X.509 Root Certificates** | S/MIME X.509-Root-CA-Zertifikate importieren und verwalten |
| **Domain keys** | openPGP und S/MIME Domänen Schlüssel importieren, synchronisieren und verwalten |
| **Customers** | Aktivieren und Einrichten einer Multi-Kunden-Konfiguration (Multitenancy). Hierbei können zum Beispiel E-Mail Domänen, Benutzerkonten oder GINA-Benutzerkonten dediziert einem zuvor definierten Kunden zugewiesen werden. |

**Referenz der Menüpunkte in der SEPPmail Konfigurationsoberfläche**

© 2015 SEPPmail AG

## 7.2 Login/Logout

Der Menüpunkt **Login** ermöglicht das Abmelden von der SEPPmail-Konfigurationsoberfläche beziehungsweise den Kennwortwechsel des angemeldeten Benutzers. In der folgenden Tabelle werden die einzelnen Parameter beschrieben.

**Sektion Login**

| Parameter | Beschreibung |
|---|---|
| User ID | Eingabe der User ID zur Anmeldung an der Administrationsoberfläche.<br>Die Anmeldung an der AdminGUI ist prinzipiell für jeden, auf SEPPmail-Appliance angelegten Benutzer möglich, welchem ein Passwort zugewiesen wurde (siehe Menü **Users** 203).<br>Ob und welche Menüs für den jeweiligen Benutzer sichtbar sind hängt von dessen Gruppenzugehörigkeit ab (siehe Menü **Groups** 213). |
| Password | Dient der Passwort Eingabe. |

**Sektion Change Password**

| Parameter | Beschreibung |
|---|---|
| **The password must:** | Gibt die Passwort Stärke der vorgegebenen Konfiguration (siehe Menü **Users** 203).<br><br>Zum Anmelden an der Konfigurationsoberfläche wählen Sie die Schaltfläche **Log in**. |
| New Password | Dient dem Passwort Wechsel des angemeldeten Bunutzers. Das Passwort muss zwei mal angegeben werden um eine fehlerhafte Eingabe zu vermeiden und den Vorgaben von "**The password must**:" entsprechen. |

| | |
|---|---|
| **Log out**. | Abmelden von der Konfigurationsoberfläche. |
| **Change Password** | Ändert das Passwort wie unter **Change Password** eingegeben. |

© 2015 SEPPmail AG

## 7.3 Home

Das Menü Home öffnet nach Anmeldung an der Konfigurationsoberfläche. Es zeigt grundlegende Informationen zum SEPPmail-System an.

#### Sektion System Status

Diese Sektion zeigt den aktuellen Systemstatus der SEPPmail-Appliance an.
Dieser sollte

**"All systems are stable and running."**

lauten. Sollten Probleme auf dem System existieren, so werden diese hier ebenso in rot angezeigt, wie eventuell wichtige, aber fehlende Konfigurationseinträge.

#### Sektion License

In dieser Sektion wird der Lizenzstatus, wie lizensierte Komponenten, deren Anzahll und Laufzeit angezeigt.

| Parameter | Beschreibung |
|---|---|
| | Wurde das System erfolgreich registriert und ist eine gültige Lizenz vorhanden, so wird hier der Status "Valid License detected" angezeigt. |
| **License Type** | Hier werden Informationen zur System- und Benutzerlizenz angezeigt. |
| **License ID** | Lizenznummer für das SEPPmail System. |
| **License Holder** | Eigentümer der SEPPmail Lizenz. |
| **Issue date** | Ausstellungsdatum der Lizenz. |
| **Comment** | Zusätzliche Informationen zur Lizenz. |
| **Encryption/Signature Licenses** | Anzahl der erworbenen Benutzerlizenzen. In Klammern wird die Anzahl bereits verwendeter Benutzerlizenzen angezeigt. |
| **Large File Management (LFM) Licenses** | Anzahl der erworbenen Benutzerlizenzen für die Funktion Large File Management. In Klammern wird die Anzahl bereits verwendeter Benutzerlizenzen angezeigt. |
| **Multitenancy** | Anzahl der erworbenen Mandantenlizenzen |
| **Software Care Pack** | Anzeige des Ablaufdatums der Lizenz für Software Updates. |
| **Device Care Pack** | Anzeige des Ablaufdatums des Device Care Packs. |
| **Protection Pack (Anti-spam/Anti-virus)** | Anzeige des Ablaufdatums der Lizenz für AntiVirus und AntiSPAM. |
| **Internal Mail Encryption** | Lizenz für interne Verschlüsselung (Active / Inactive). |

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| **Self-Service password management** | Lizenz für Self-Service passwort management (Active / Inactive). |

**Sektion System**

Zeigt die Systemdaten der Appliance an.

| Parameter | Beschreibung |
|---|---|
| **Device ID** | Gerätelizenznummer |
| **Appliance Type** | Typ der aktuellen Appliance, zum Beispiel SEPPmail 5000 (VMware Virtual Appliance). |
| **Firmware Version** | Aktuell auf dem System installierte Softwareversion. |
| **Uptime** | Laufzeit des Systems nach dem letzen Neustart. |

**Sektion Anti-Virus**

Zeigt den Status des integrierten Virenscanners an

| Parameter | Beschreibung |
|---|---|
| **Inactive** | Falls das Protection Pack (VSPP) nicht lizensiert wurde ist dies die einzige Anzeige der Sektion. |
| **ClamAV Engine** | Anzeige der ClamAV Scan Engine Version |
| **Signature Version** | Anzeige der ClamAV Virensignatur Version |
| **Signature Date** | Anzeige des ClamAV Virensignatur Datums |

**Sektion Mail statistics**

Zeigt eine Kurzübersicht der verarbeiteten E-Mail an.

| Parameter | Beschreibung |
|---|---|
| **Mails Processed** | Anzahl aller insgesamt vom System übertragenen E-Mails (empfangen, gesendet). |
| **Mails Processed (S/MIME)** | Anzahl aller insgesamt via S/MIME verarbeiteten E-Mails (entschlüsselt, verschlüsselt). |

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| **Mails Processed (openPGP)** | Anzahl aller insgesamt via openPGP verarbeiteten E-Mails (entschlüsselt, verschlüsselt). |
| **Mails Processed (DOMAIN)** | Anzahl aller insgesamt via Domänen Verschlüsselung verarbeitenten E-Mails (entschlüsselt, verschlüsselt). |
| **GINA Mails** | Anzahl aller insgesamt versendeten Secure Webmails über das GINA-Subsystem. |
| **Mails currently in queue** | Anzahl aller E-Mails in der Warteschlange. |

**Sektion Disk statistics**

Zeigt die Auslastung der einzelnen Systempartitionen an.

| Parameter | Beschreibung |
|---|---|
| **Database** | Zeigt die Auslastung des Datenbank Volumes im System |
| **Mail queue** | Zeigt die Auslastung des E-Mail Warteschlangen Volumes im System |
| **Log** | Zeigt die Auslastung des Volumes für die Log-Dateien im System |
| **temp** | Zeigt die Auslastung des Volumes für temporäre Dateien im System |
| **LFM store** | Zeigt die Auslastung des Volumes für die Large File Management Volume im System sofern dieses Feature lizensiert wurde |

© 2015 SEPPmail AG

## 7.4 System

Das Menü **System** kann in zwei Ansichten betrachtet werden. Die grundlegenden Basiseinstellungen sind in der Ansicht **Normal View** zu sehen. Diese Ansicht ist die Standardansicht bei Aufruf des Menüs. Eine vollständige Übersicht aller Einstellungen ist in der Ansicht **Advanced View** zu sehen.

**Advanced View**

Durch betätigen der Schaltfläche **Advanced View** werden die erweiterten Parameter angezeigt. Um die erweiterte Darstellung des Menüpunkts **System** wieder zusammenzufassen ist in der Erweiteren Darstellung die Schaltfläche **Normal View** zu betätigen.

**Normal View**

In diesem Menü werden die wichtigsten Parameter der LAN-Anbindung des SEPPmail-Systems eingerichtet. Die hier eingetragenen Daten dienen auch als Grundeinstellung für viele weitere Einstellungen des SEPPmail-Systems.

Die folgenden Tabellen beschreiben den **Advanced View**, da dieser alle Einstellungen des **Normal View** beinhaltet.

**Sektion Comment** (optional)

Eingabefelder zur Beschreibung beziehungsweise zur Identifikation des SEPPmail-Systems. Diese Parameter werden zum Beispiel als Betreff in der automatischen Datensicherung sowie von SNMP verwendet. Ansonsten dienen Sie lediglich der Beschreibung. Die Einträge sind frei wählbar und jeweils optional.

| Parameter | Beschreibung |
|---|---|
| **System Description** | Kurzbeschreibung des Systems. |
| **System Location** | Standort des Systems |
| **System Object ID** | Eigene ID des Systems |
| **System Contact** | Ansprechperson für das System |
| **System Name** | Name des Systems |

**Sektion IP Addresses**

| Parameter | Beschreibung |
|---|---|
| **Interface 1** | Eingabemaske für IP-Adresse mit Subnetzmaske und den Medientyp der physischen Netzwerk Schnittstelle **LAN1** bzw. **eth0**. In den meisten Umgebungen sollte der Medientyp auf dem Standardwert **autoselect** belassen bleiben.<br><br>Für jede physisch vorhandene Netzwerk-Schnittstelle wird jeweils eine Schnittstellen-Konfiguration angezeigt. Die hier angezeigte Schnittstellen-Nummer entspricht der folgenden Netzwerk-Schnittstelle: |

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| | **Interface 1 - LAN1** bzw. **eth0** oder auch **vic0** bei virtuellen Appliances |
| **Interface 2 - 4**<br>(optional) | Wie bei **Interface 1** jedoch jeweils für<br>**Interface 2 - LAN2** bzw. **eth1** oder auch **vic1**<br>**Interface 3 - LAN3** bzw. **eth2** oder auch **vic2**<br>**Interface 4 - LAN4** bzw. **eth3** oder auch **vic3** |
| **Team / bond interfaces**<br>(optional) | Durch Verwendung dieser Einstellung können mehrere Interfaces gebündelt und logisch wie eines verwendet werden. Dabei gibt es unterschiedliche Verfahren:<br>• broadcast (Ausfallsicherheit)<br>Nutzung meherer Switches gleichzeitig möglich.<br>• failover (Ausfallsicherheit)<br>Nur ein Interface ist aktiv, bei Ausfall wird auf das nächste übergegangen. Nutzung meherer Switches möglich.<br>• lacp / 802.3ad (Lastverteilung, Ausfallsicherheit)<br>Bündelung mehrerer Schnittstellen zur Erreichung höherer Bandbreiten. Anbindung an nur einen Switch mit entsprechender Protokollunterstützung möglich.<br>• loadbalance (Lastverteilung)<br>Jeder Gegenstelle im Netzwerk ein zu nutzendes Interface zugewiesen.<br>• roundrobin (Lastverteilung, Ausfallsicherheit)<br>Verfügbare Interfaces werden in Senderichtung wechselweise genutzt, in Empfangsrichtung kann max. die Geschwindigkeit einer einzelnen Interface genutzt werden. |
| **Custom hosts file entries:**<br>(optional) | Zum Durchführen einer lokalen Namensauflösung muss in diesem Feld eine Kombination von IP-Adressen und Hostname/n eintragen werden.<br><br>**Format:**<br>62.2.145.228 update seppmail.ch support.seppmail.ch<br>193.239.220.29 pool.ntp.org |

**Sektion IP ALIAS Addresses** (optional)

Werden mehrere SEPPmail-Appliances in einem Clusterverbund betrieben, so können diese gemeinsam über eine oder auch mehrere virtuelle IP-Adressen angesprochen werden. Die Stellung der einzelnen Maschine innerhalb dieses Verbundes wird über die Priorität (Priority:) definiert.

**Hinweis:**

Um die Funktion des CARP-Protokolls - welches die Basis für das Bereitstellen virtueller IP-Ardressen bildet - zu gewährleisten, müssen bei virtuellen Appliances gegebenenfalls folgende Einstellungen vorgenommen werden:

- **Microsoft Hyper-V**
  Option "Spoofing von MAC-Adressen aktivieren" in der Konfiguration der virtuellen Netzwerkkarte aktivieren.
  Diese Option ist in den Hyper-V Einstellungen der virtuellen Maschine unter "Ältere Netzwerkkarte -> Erweiterte Features" zu finden.
- **ESX**
  "promiscous mode" in der Konfiguration der virtuellen Netzwerkkarte aktivieren.
  Diese Option ist in den ESX Einstellungen wie folgt vorzunehmen:
  1. Im "vSphere Web Client" zum entsprechenden "Host" navigieren

© 2015 SEPPmail AG

2. Anwählen der Registerkarte "Verwalten"
3. Anwählen "Virtuelle Switches" in der Auswahl rechts der Registerkarte
4. Anwählen des umzustellenden "Switches"
5. Anwählen der Option "Einstellungen bearbeiten" durch Klick auf das Bleistift-Symbol
6. Anwählen "Sicherheit" in der Auswahl rechts des Fensters
7. Option "Promiscuous-Modus" über das Auswahlmenü auf "Aktzeptieren" stellen und mit "OK" bestätigen

<table>
<tr><th>Parameter</th><th>Beschreibung</th></tr>
<tr><td>IP Alias 0 - 3</td><td>An dieser Stelle können virtuelle IP-Adressen definiert werden, welche in der Regel bei Clusterconfigurationen zum Einsatz kommen (siehe Menü Cluster 195).<br>Hierzu ist es erforderlich für jeden Alias<br>1. eine IP-Adresse<br>2. die Netzwerkmaske<br>3. die VHID (Virtual Host Identification)<br>4. das Interface an welches der Alias gebunden werden soll<br>5. die Priorität der Schnittstelle im Verbund (Primary, Secondary, Backup)<br>anzugeben.<br><table><tr><th>IP-Adresse</th><th>Subnetz</th><th>VHID</th><th>Interface</th><th>Priority</th></tr><tr><td>Angabe der virtuellen IP-Adresse auf welche die Systeme gemeinsam reagieren sollen</td><td>zum Beispiel /24 für C-Klasse</td><td>Die VHID (Virtual Host Identification) muss bei allen Maschinen, welche ebenfalls auf die eingetragene virtuelle IP reagieren sollen gleich sein.</td><td>Angabe der Netzwerk Schnittstelle (siehe Sektion IP Addresses), an welche die virtuelle IP gebunden werden soll.</td><td>Stellung der einzelnen Maschine innerhalb dieses Verbundes.</td></tr></table></td></tr>
</table>

**Sektion SMTP Loadbalancer** (optional)

Dient der Lastverteilung bei Betrieb eines Clusters.

| Parameter | Beschreibung |
|---|---|
| **Enable Load balancer** | Aktiviert die SMTP Loadbalancer Funktion.<br>Das SMTP Loadbalancing reicht erst nach erreichen eines hohen Auslastungsgrades - Auslöser ist die Anzahl (10) der gleichzeitigen Verbindungen - E-Mails an die eingetragenen Clusterpartner weiter. Hierdurch wird die Fehleranalyse erleichtert, da eine Sichtung der Logs im Regelfall auf der Hauptmaschine ausreiichend ist. |

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| Distribute load to the following cluster members | An dieser Stelle werden die IP-Adressen der Clusterpartner für das Loadbalancing eingegeben. Die IP-Adressen werden im Eingabefeld durch ein Leerzeichen getrennt. |

**Sektion Name**

Der Name des Systems setzt sich aus dem Hostnamen und der Domäne zusammen. zum Beispiel securemail.seppmail.ch
**Diese Einstellungen sind die interne Sicht, sie müssen also nicht den Daten, wie sie vom Internet her Gültigkeit hätten, entsprechen.**

| Parameter | Beschreibung |
|---|---|
| Hostname | Eingabe des Hostnamens des SEPPmail Systems ein. zum Beispiel securemail |
| Domain | Eingabe der Domäne des SEPPmail Systems ein. zum Beispiel seppmail.ch |

**Sektion Routing**

| Parameter | Beschreibung |
|---|---|
| **Default Gateway** | Angabe der Gateway-Adresse passend zum Netzwerksegment (IP und Netzmaske wie sie unter **IP Addresses** eingegeben wurden). An dieses Gateway werden alle Datenpakete weitergeleitet, welche an Zieladressen ausserhalb des lokalen Netzwerksegments gesendet werden sollen. |
| **Static Routes** (optional) | Sollten Verbindungen zu Netzen hergestellt werden müssen, welche nicht über das **Default Gateway** erreichbar sind, so können an dieser Stelle die entsprechenden Netze mit ihrem Subnetz jeweils unter "**Destination**" und das jeweils dort hin führende "**Gateway**" angegeben werden. Diese statischen IP-Routen haben Priorität vor der Verwendung des Standard-Routers (Default Gateway).<br>Nach dem Speichern einer statischen Route wird jeweils ein weiteres Eingabefeld eingeblendet. |

**Sektion DNS**

| Parameter | Beschreibung |
|---|---|
| **Use built-in DNS Resolver** | Bei diesem Parameter versucht das System die DNS-Namensauflösung immer mit Hilfe der DNS-Root-Nameserver im Internet. Ist dieser Parameter ausgewählt, so kann die Auflösung von DNS-Namen ggf. sehr lange dauern und die Reaktion des SEPPmail Systems dadurch verzögert werden. |

© 2015 SEPPmail AG

<table>
<tr><td colspan="2">Use the following DNS Servers</td><td>DNS-Anfragen für Adressen, für welche die SEPPmail nicht selbst zuständig ist, werden an übergeordnete DNS-Name-Server weitergeleitet. Dazu sollte SEPPmail die DNS-Anfrage zunächst an einen internen DNS-Server im eigenen Netzwerk oder die DNS-Server Ihres Internet Providers weitergeben, die Sie hier spezifizieren können.</td></tr>
<tr><td></td><td>Primary</td><td>Gehen Sie hier den ersten DNS-Name-Server ein an den SEPPmail DNS-Anfragen weiterleiten soll.</td></tr>
<tr><td></td><td>Alternate 1<br>(optional)</td><td>Ist der primäre DNS-Name-Server nicht verfügbar oder antwortet nicht wird die DNS-Anfrage an den hier eingetragenen, alternativen DNS-Name-Server weitergeleitet.</td></tr>
<tr><td></td><td>Alternate 2<br>(optional)</td><td>Sind weder der primäre noch der erste alternative DNS-Name-Server verfügbar, so wird die DNS-Anfrage an den hier eingetragenen, zweiten alternativen DNS-Name-Server weitergeleitet.</td></tr>
<tr><td></td><td>Search Domain(s)</td><td>Geben Sie hier eine Suchliste mit Domänen Namen an, welche bei einer DNS-Anfrage nacheinander abgefragt werden.</td></tr>
<tr><td></td><td>add local zone<br>(optional)</td><td>Lokale Zonen werden verwendet, wenn jeweils mehrere Forwarding- und/ oder SMTP-Server angesprochen werden sollen, für das Auflösen der hierfür benötigten MX-Records jedoch kein lokaler DNS-Server zur Verfügung steht.<br>Nach dem Speichern werden jeweils ein weitere Eingabefelder eingeblendet.<br><br>In den unten dargestellten Beispiel Eintragungen würde für die Domäne pseudo.local vorrangig in mail1.pseudo.local mit der IP-Adresse 10.0.0.11 aufgelöst da dieser die Präferenz 10 aufweist. Sollte der Server mail1.pseudo.local nicht erreichbar sein, wird der Eintrag mit der Präferenz 20, also mail2.pseudo.local mit der IP-Adresse 10.0.0.12 verwendet.
<table>
<tr><td>Domain name:</td><td colspan="5">Pseudo Domänen Name, welcher intern in der SEPPmail-Appliance als MX-Record aufgelöst werden soll, zum Beispiel pseudo.local.</td></tr>
<tr><td>host:</td><td>Hostname, zum Beispiel mail1</td><td>mx:</td><td>Präferenz, zum Beispiel 10</td><td>ip:</td><td>IP-Adresse des ersten E-Mail-Servers, zum Beispiel 10.0.0.11</td></tr>
<tr><td>host:</td><td>Hostname, zum Beispiel mail2</td><td>mx:</td><td>Präferenz, zum Beispiel 10</td><td>ip:</td><td>IP-Adresse des zweiten E-Mail-Servers, zum Beispiel 10.0.0.12</td></tr>
</table>
</td></tr>
</table>

**Sektion GUI Protocol**

Definiert die Einstellungen für den Zugriff auf die Adminoberfläche.

| Parameter | Beschreibung |
|---|---|
| **HTTP Port** | Aktivieren Sie diesen Parameter, um den unverschlüsselten Zugriff via HTTP Protokoll auf die Konfigurationsoberfläche zu ermöglichen. Geben |

© 2015 SEPPmail AG

| | |
|---|---|
| | Sie dazu einen entsprechenden TCP/Port (im Standard 8080) an.<br>**Um Sicherheitsrisiken zu minimieren ist diese Option im Standard deaktiviert.** |
| **HTTPS Port** | Aktiviert den verschlüsselten Zugriff via HTTPS Protokoll auf die Konfigurationsoberfläche zu ermöglichen. Geben Sie dazu einen entsprechenden TCP/Port (im Standard 8443) an.<br>Dies ist der Standard Zugriff auf die SEPPmail Konfigurationsoberfläche. |
| Admin GUI Session timeout: | Zeit in Sekunden bis zum automatischen Logout aus der Konfigurationsoberfläche bei Inaktivität. |

**Sektion GINA-https Protocol**

Definiert die Einstellungen für den Zugriff auf das GINA-Webinterface.

| Parameter | Beschreibung |
|---|---|
| **HTTP Port** | Aktivieren Sie diesen Parameter, um den unverschlüsselten Zugriff via HTTP Protokoll auf die Webmail-Schnittstelle des SEPPmail Systems zu ermöglichen. Geben Sie dazu einen entsprechenden TCP/Port (im Standard 80) an.<br> <br>**Hinweis:**<br>Verwenden Sie das HTTP-Protokoll nicht für einen Zugriff auf die Webmail-Schnittstelle aus dem Internet oder aus einem anderen unsicheren Netzwerk. Hierdurch würde das Protokollieren von Webbrowserverbindungen zur Webmail-Schnittstelles des SEPPmail durch unbefugte Dritte ermöglicht.<br>Diese Einstellung wird in der Regel nur dann benötigt, wenn bereits eine vorgeschaltete Komponente den SSL-Tunnel zum GINA-Webinterface terminiert. |
| **HTTPS Port** | Aktivieren Sie diesen Parameter, um den verschlüsselten Zugriff via HTTPS Protokoll auf die Webmail-Schnittstelle des SEPPmail Systems zu ermöglichen. Geben Sie dazu einen entsprechenden TCP/Port (im Standard 443) an. |
| **Enable local https proxy, redirect unknown requests to** (optional) | Aktivieren Sie diesen Parameter, um den Zugang zum Webmail Subsystem (GINA Webinterface) nicht mehr direkt sondern über den lokalen SEPPmail Reverse-Proxy zu aktivieren. Alle nicht für das Webmail bestimmten Anfragen werden dadurch an die eingetragene URL weitergeleiten.<br>Hierdurch kann zum Beispiel der Zugang zu einem internen OWA-Server (Outlook Web Access) gewährleistet werden. Ebenfalls können ActiveSync Verbindungen zum internen MS-Exchange Server durch den Reverse-Proxy weitergeleitet werden. |

**Sektion Console Login** (optional)

Definiert die Einstellungen für den Zugriff auf die Console der Appliance.

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| **Disable console root login** | Aktivieren Sie diesen Parameter, so wird der Konsolenzugang am SEPPmail System gesperrt.<br><br>**Hinweis:**<br>Bitte beachten Sie beim Aktivieren dieses Parameters, dass in diesem Fall ein gewollter Zugang zum System im Fehlerfall ebenfalls nicht mehr möglich ist. |

**Sektion Syslog Settings** (optional)

Ermöglicht die Weiterleitung von Log-Einträgen an einen Syslog Server.

| Parameter | Beschreibung |
|---|---|
| Forward maillog and authlog to this syslog server | Hostname oder IP-Adresse eines Syslog-Servers im LAN an welchen die SEPPmail die Mail- und Auzuthentifizierungs- Log-Protokolle zusätzlich senden soll. Als Zielport wird UDP/514 verwendet. |
| Forward GUI audit log to this syslog server | Hostname oder IP-Adresse eines Syslog-Servers im LAN an welchen die SEPPmail die Log-Protokolle der Aktionen aus der AdminGUI zusätzlich senden soll. Als Zielport wird UDP/514 verwendet. |

**Sektion Log Cleanup** (optional)

| Parameter | Beschreibung |
|---|---|
| **Automatically delete log archives older than ? days** | Löscht Log-Archive automatisch nach der eingestellten Anzahl von Tagen. Minimum sind 30 Tage, Maximum 3640 Tage (10 Jahre)<br>Durch das automatische löschen der Log-Archive kann ein "vollaufen" der Log-Partition vermieden werden. |

**Sektion Proxy Settings** (optional)

Hier müssen nur dann entsprechende Einstellungen vorgenommen werden, wenn ein direkter Zugriff der Appliance per SSH (TCP Port 22) in das Internet nicht möglich ist.

| Parameter | Beschreibung |
|---|---|
| **Proxy Server** | Hostname oder IP-Adresse des Proxy-Servers, über welchen die SSH Kommunikation geleitet werden soll. |
| **Proxy Port** | Ziel-Port des Proxy-Servers, zum Beispiel 8080 oder 8081 |
| **Proxy User** (optional) | Benutzername für die Anmeldung am Proxy-Server sofern diese notwendig ist. |

© 2015 SEPPmail AG

| | |
|---|---|
| **Proxy Password** (optional) | Kennwort für die Anmeldung am Proxy-Server |
| **Use direct connection on port 22 outgoing (preferred)** | Aktivieren Sie diese Option, wenn eine SSH-Verbindung direkt und ohne Umweg über einen Proxy-Server ins Internet möglich ist. |
| **Connect through SOCKS 4 proxy** | Aktivieren Sie diese Option, um SSH-Verbindungen durch einen generischen SOCKS-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang via SSH ins Internet reglementiert ist, für dass SEPPmail System aber die Verbindung über einen SOCKS-Proxy (Version 4) ins Internet möglich ist. |
| **Connect through SOCKS 5 proxy** | Aktivieren Sie diese Option, um SSH-Verbindungen durch einen generischen SOCKS-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang via SSH ins Internet reglementiert ist, für dass SEPPmail System aber die Verbindung über einen SOCKS-Proxy (Version 5) ins Internet möglich ist. |
| **Connect through HTTP proxy** | Aktivieren Sie diese Option, um SSH-Verbindungen durch einen HTTP-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang via SSH ins Internet reglementiert ist, für dass SEPPmail System aber die Verbindung über einen HTTP-Proxy ins Internet möglich ist. |
| **Connect through Telnet proxy** | Aktivieren Sie diese Option, um SSH-Verbindungen durch einen Telnet-Proxy zu tunneln. Diese Option kann verwendet werden, wenn der direkte Zugang via SSH ins Internet reglementiert ist, für dass SEPPmail System aber die Verbindung über einen Telnet-Proxy ins Internet möglich ist. |
| **Use port 80 instead of 22** | Aktivieren Sie diese Option, wenn eine HTTP-Verbindung direkt ins Internet möglich ist. Die SSH-Verbindung verwendet dann den Port TCP 80 (HTTP) statt TCP 22 (SSH). |

**Sektion Time zone**

| Parameter | Beschreibung |
|---|---|
| **Auswahl der Zeitzone** | Wählen Sie im Auswahlmenü die für den Standort des SEPPmail Systems gültige Zeitzone aus. Der Wechsel zwischen Sommer- und Winterzeit wird automatisch durchgeführt. |

**Sektion Time and Date**

| Parameter | Beschreibung |
|---|---|
| **No time sync** | Mit dieser Einstellung wird ausschliesslich die interne Systemzeit verwendet. Diese kann über **Set date and time manually** entsprechend eingestellt werden. Ein automatische Abgleich mit anderen Systemen findet nicht statt! |
| **Automatically synchronize with an NTP server** | Bei dieser Option werden Datum und Uhrzeit gegen den unter "Server" angegebenen Zeitserver über das Protokoll NTP, Zielport TCP 123, synchronisiert. |

© 2015 SEPPmail AG

| | |
|---|---|
| | **Hinweis:** Diese Option ist für die Einrichtung eines Clusters auf allen Cluster Membern zwingend erforderlich. |
| Server | Hostname oder IP-Adresse eines Zeitservers. Dieser kann sich in Ihrem Firmennetzwerk oder im Internet befinden. |
| **Set date and time manually** | Hier können Sie die Werte für das aktuelle Datum und die aktuelle Uhrzeit manuell eingeben. |
| Date | aktuelles Datum im Format: dd.mm.yyyy |
| Time | aktuelle Uhrzeit im Format: hh:mm:ss |

**Sektion SNMP Daemon** (optional)

Die hier vorgenommenen Änderungen werden erst nach einem Neustart der SEPPmail-Appliance aktiv.
Wird weder bei "**snmp v1/2 Read-only Community" noch bei "snmp v1/2 Read-write Community" eine Eingabe gemacht, so wird SNMP v1/2 deaktiviert.**
**Für die SNMP v3 Verschlüsselung wird AES, für die Authentifikation SHA als Algorithmus verwendet**

| Parameter | Beschreibung |
|---|---|
| **Enable SNMP** | Aktivieren und deaktivieren des SNMP Deamon auf dem SEPPmail System. Nach Aktivierung des SNMP Protokols können Sie mit SNMP-Tools wie zum Beispiel snmpwalk Informationen Ihres SEPPmail Systems abrufen. |
| Listen Address | IP-Adresse zu der sich das SNMP-Monitoring verbindet. Dies ist in der Regel die IP-Adresse der SEPPmail-Appliance. |
| snmp v1/2 Read-only Community | Passwort für den Nur-Lese Zugriff auf die SNMP-Daten. |
| snmp v1/2 Read-write Community | Passwort für den Schreib-Lese Zugriff auf die SNMP-Daten. |
| snmp v3 user | Benutzername für den SNMP v3 Zugriff |
| snmp v3 password | Passwort für den SNMP v3 Zugriff. Dieses muss mindestens acht Zeichen lang sein. |
| **Download MIBs** | Über diesen Link können Sie Management Information Bases (MIB) des SEPPmail Systems als ZIP-Datei herunterladen. |

**Sektion VMware Tools** (optional)

© 2015 SEPPmail AG

| Parameter | Beschreibung |
| --- | --- |
| **Enable VMware tools (restart to activate setting)** | Im Standard wird ein Kernel mit aktivierten VMware Tools verwendet. Da diese Tools in einigen wenigen Konstellationen mit ESX zu Problemen führen können, besteht die Möglichkeit diese zu deaktivieren.<br>Eine hier vorgenommene Änderung wird erst nach einem Neustart der SEPPmail-Appliance aktiv. |

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

© 2015 SEPPmail AG

## 7.5 Mail System

Im Menüpunkt **Mail System** werden grundlegende Einstellungen des SEPPmail E-Mail-Systems vorgenommen.

### Sektion Managed Domains

Definiert die E-Mail-Domänen welche verwaltet werden sollen.

| Spalte | Beschreibung |
|---|---|
| **Domain Name** | Liste aller auf dem SEPPmail-System angelegten E-Mail Domänen. Für diese Domänen werden E-Mails angenommen und entsprechend verarbeitet. |
| **Server IP Address** | Zeigt die IP-Adresse, den Hostnamen oder den MX-Eintrag des internen Groupware Systems an, an welches eingehende E-Mails für den jeweils oben genannten **Domain Name** weitergeleitet werden. |
| **Server Port** | Zeigt den Port an, auf welchem die jeweils oben genannten **Server IP Address** E-Mails für den zugehörigen **Domain Name** annimmt. |
| **TLS level** | Zeigt an, welche Art der TLS-Transportverschlüsselung für die jeweilige E-Mail Domäne verwendet wird. |
| **GINA Settings** | Zeigt das GINA-Profil an, welches für jeweilige E-Mail Domäne festgelegt wurde (siehe auch Edit GINA Settings 165). |
| **Disclaimer Settings** (optional) | Zeigt an, welcher Disclaimer an ausgehende E-Mails der jeweiligen E-Mail Domäne angefügt werden soll (siehe auch Mail Processing 147 Edit Disclaimer). |
| **Customer** (optional) | Name des Kunden, dem diese E-Mail Domäne zugeordnet wurde (siehe auch Customers 223). |
| **Add Domain...** | Wählen Sie diese Schaltfläche, um weitere E-Mail Domänen hinzuzufügen. Diese E-Mail Domänen müssen passend sein zu den E-Mail- Adressen Ihres Unternehmens. Weitere Informationen zur Verwaltung von E-MailDomänen erhalten Sie im Kapitel Add/Edit Managed Domain 136 . |
| **Automatically create and publish S/MIME domain keys for all domains** | Dieser Parameter bewirkt, dass für alle über die Schaltfläche **Add Domain...** neu hinzugefügten E-Mail Domänen automatisch ein selbst signiertes X.509 S/MIME Domänen Zertifikat erzeugt und an einen zentralen Updateservice übertragen wird. Dieses neu erzeugte S/MIME Domänen Zertifikat (also ausschliesslich der öffentliche Schlüssel !!!) für Ihre E-Mail Domänen wird danach automatisch an alle SEPPmail-Systeme verteilt, so dass alle Unternehmen die ein SEPPmail-System betreiben ohne weiteren Aufwand E-Mails ausschliesslich verschlüsselt untereinander austauschen. Dieser Service ist bereits in der Basis-Lizenz enthalten und erfordert keine zusätzlichen Encryption-Lizenzen.<br><br>**Hinweis:**<br>Die Genehmigung der Veröffentlichung des S/MIME-Domainzertifikats muss bei SEPPmail nach Erstellung der Managed Domain nochmals explizit erteilt werden.<br>Soll nicht am Managed Domain Service teilgenommen werden, so ist diese Option zu deaktivieren bevor die erste E-Mail Domäne angelegt wird. Das S/MIME-Domain- |

© 2015 SEPPmail AG

| Spalte | Beschreibung |
|---|---|
| | Zertifikat wird dann nicht automatisch erzeugt. |
| **Fetch Mail from remote POP3 server** | Dieser Parameter bewirkt, dass das im Benutzerkonto eingerichtete POP3-Konto durch SEPPmail jeweils in einem Zeitintervall von drei Minuten abgeholt wird. Die so abgeholten E-Mails werden im Anschluss durch das SEPPmail System verarbeitet und an den entsprechenden "Forwarding Server" (**Server IP Address**) weitergeleitet.<br>Siehe auch Kapitel **Benutzerdetails** 204. |
| **Verify recipient addresses using SMTP-Lookups** | Dieser Parameter bewirkt, dass die E-Mail-Adresse des Empfängers vorab bei dem für die E-Mail Domäne eingerichteten E-Mail-Server an den die E-Mails weitergeleitet werden überprüft wird. Verläuft die Prüfung der Empfänger E-Mail-Adresse nicht erfolgreich, wird die Annahme der E-Mail vom SEPPmail System verweigert.<br> <br>**Hinweis:**<br>Sollte der als "Forwarding Server" (**Server IP Address**) angezeigte Server nicht der E-Mail Server, sondern eine zwischengelagerte Komponente sein, so ist bei Aktivieren dieses Parameters mit Problemen zu rechnen. |

**Sektion Outgoing Server**

Definiert die Art der Weiterleitung ausgehender E-Mails.

| Parameter | Beschreibung |
|---|---|
| **Use built-in mail transport agent** | Dieser Parameter bewirkt, dass ausgehende E-Mails in Richtung Internet direkt durch das SEPPmail System an den Ziel E-Mail-Server des E-Mail-Empfängers zugestellt wird. Die Appliance muss für diese Einstellung direkt aus dem Internet per MX-Record erreichbar sein.<br> <br>**Hinweis:**<br>Bei Verwenden dieser Einstellung wird dringend empfohlen das optionale Protection Pack (VSPP) zu lizensieren und aktivieren, sofern für den eingehenden E-Mail Verkehr nicht etwa ein externer AntiSpam-Dienst vorgeschaltet ist. Andernfalls ist mit erheblichen Beeinträchtigungen, bis hin zum Erliegen des Mailflusses durch SPAM-Attacken zu rechnen. |
| **Use the following SMTP server** | Möchten Sie ausgehende E-Mails in Richtung Internet nicht direkt zustellen empfielt sich das Verwenden eines E-Mail-Relay-Servers (Smart Host). Alle ausgehenden E-Mails werden an diesen E-Mail-Relay-Server übertragen, welcher dann Ihre E-Mails in Richtung Empfänger weiterleitet. Der E-Mail-Relay-Server kann ein Interner Server aber auch ein Server bei Ihrem E-Mail Provider sein. |
| Server name | Als Eingabe wird folgendes aktzeptiert:<br>IP-Adresse — einzelne IP-Adresse (in eckige Klammern [ ] zu setzen). |

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| | Hostname: wird ein Hostname verwendet, so ist dieser in eckige Klammern [ ] zu setzen. Namen ohne Klammern werden als MX-Eintrag behandelt<br>MX-Name: MX-lookup wird ausgeführt<br>**Es wird der Port 25 (SMTP) verwendet. Die Angabe eines alternativen Ports ist nicht zulässig.** |
| **Server requires authentication** | E-Mail-Relay-Server bei einem Provider benötigen vor dem Übertragen von E-Mails meist eine Anmeldung. Verwenden Sie hierzu die entsprechenden Anmeldedaten. |
| User ID | Geben Sie hier bitte den Benutzernamen zur Anmeldung ein. |
| Password | Geben Sie hier bitte das Kennwort zur Anmeldung ein. |

**Sektion TLS settings** (optional)

An dieser Stelle werden TLS-Verbindungen nach aussen aufgelistet beziehungsweise eingerichtet. Wurde in der Sektion **Outgoing Server** die Option **Use the following SMTP server** gewählt, so kann hier zu dem oder den unter Server name eingetragenen Server(n) TLS-Verschlüsselung eingerichtet werden. Wurde die Option **Use built-in mail transport agent** gewählt, so kann hier bei Bedarf zu beliebigen E-Mail Servern im Internet ein TLS-Verbindung konfiguriert werden, sofern diese TLS unterstützen.

**Hinweis:**
Wird hier keine Konfiguration vorgenommen, so gilt die Einstellung "may", das heisst die SEPPmail-Appliance wird zu allen Kommunikationspartnern eine TLS-verschlüsselte Verbindung aufbauen, sofenr die Gegenstelle dies unterstützt.
**Für die TLS Verschlüsselung wird das unter SSL eingebundene Zertifikat verwendet**.

| Parameter | Beschreibung |
|---|---|
| **Domain Name** | Liste aller auf dem SEPPmail-System angelegten E-Mail Domänen, für welche eine TLS-Verbindung konfiguriert wurde auf. |
| **Server IP Address** | Zeigt die IP-Adresse, den Hostnamen oder den MX-Eintrag für den jeweils oben genannten **Domain Name** an. |
| **Server Port** | Zeigt den Port an, welcher für die TLS-verschlüsselte Verbindung zur oben genannten **Server IP Address** verwendet wird. Im Standard ist das 25. |
| **TLS level** | Zeigt an, welche Art der TLS-Transportverschlüsselung von der SEPPmail Appliance zum angegebenen E-Mail-Server für die jeweilige E-Mail Domäne verwendet wird. |
| **GINA Settings** | Zeigt das GINA-Profil an, welches für diese E-Mail Domäne festgelegt wurde. |

Um bestehende TLS-Verbindungen zu verwalten ist auf den jeweiligen "Domain Name" zu klicken.

© 2015 SEPPmail AG

Neue TLS-Verbindungen werden über die Schaltfläche **Add TLS Domain...** eingerichtet.
Weitere Informationen zur Verwaltung von TLS E-Mail Domänen erhalten Sie im Kapitel **Add TLS Domain** 143.

### Sektion SMTP settings

Definiert spezifische Einstellungen für das SMTP-Protokoll.

| Parameter | Beschreibung |
|---|---|
| max. message size (kb) (optional) | Geben Sie in diesem Feld die maximale Grösse einer E-Mail in Kilobyte ein die durch das SEPPmail-System übertragen werden darf. E-Mails die diese Grösse überschreiten werden abgelehnt. Wird hier eine Beschränkung festgelegt, so ist darauf zu achten, wie diese gegebenenfalls mit dem Groupware Server beziehungsweise des optional zum Internet hin vorgeschaltenen Systems zusammenpasst. Sollte die SEPPmail-Appliance über den MX-Record im Internet direkt angesprochen werden ist der Eintrag eines Limits zwingend. Dieses darf die angezeigte Grosse (siehe **Note: cannot exceed xxxxx kB**) nicht überschreiten. |
| Postmaster address | Geben Sie die E-Mail Adresse des lokalen Administrators des SEPPmail-Systems ein. Alle vom SEPPmail erzeugten Statusmeldungen wie zum Beispiel Watchdog Meldungen werden an diese E-Mail-Adresse gesendet.<br> <br>**Hinweis:**<br>Die Postmaster address muss gesetzt werden um Systembenachrichtigungen empfangen zu können. |
| SMTP server HELO string (optional) | Festlegen, welchen Namen SEPPmail beim Versand von E-Mails im HELO/ EHLO-Befehl verwenden soll.<br>Die Appliance wird sich im Normalfall mit dem unter **System** 119 **Name** eingegebenen Namen melden. Handelt es sich hierbei um einen aus dem internet nicht erreichbaren Namen (zum Beispiel Domäne ".local") so kann es erforderlich sein, hier den aus dem Internet erreichbaren Namen (FQDN) einzutragen. Somit wird gewährleistet, dass Mailserver welche mit der Einstellung "Require fully qualified domain name in HELO command" arbeiten E-Mails von der SEPPmail-Appliance auch annehmen. Das heisst die Einstellung ist meist nur dann relevant, wenn in der Sektion **Outgoing Server** dieses Menüs die Einstellung **Use built-in mail transport agent** aktiv ist. |
| SMTP bind address (use with care!) (optional) | Festlegen der IP-Adresse einer Netzwerk-Schnittstelle, über die alle E-Mails empfangen werden (normalerweise nicht notwendig).<br>Die SEPPmail-Appliance bindet im Normalfall alle vorhandenen Netzwerk Interfaces. Sind mehrere Interfaces aktiv, jedoch nur eines davon soll für SMTP Verbindungen zur Verfügung stehen, so kann dessen IP-Adresse hier eingetragen werden.<br> <br>**Hinweis:**<br>Fällt das Interface der hier eingetragenen IP-Adresse aus, so ist die Appliance per SMTP nicht mehr erreichbar. Somit würde auch der E-Mail Verkehr unterbrochen. |

© 2015 SEPPmail AG

**Sektion Relaying**

Definition der für den Versand von E-Mails in das Internet berechtigten Systeme.

| Parameter | Beschreibung |
|---|---|
| Relaying allowed: | Geben Sie hier die IP-Adresse oder das Subnetz an, von welcher/m das SEPPmail System annehmen soll.<br>Nach dem Speichern werden jeweils ein weitere Eingabefelder eingeblendet.<br> <br>**Hinweis:**<br>In der Regel sind hier die IP-Adressen der Forwarding Server (siehe **Managed Domains** beziehungsweise Kapitel **Add/ Edit Managed Domain** 136) zu berechtigen.<br>Um ein sogenanntes "open relay" zu verhindern, sollte hier keinesfalls der SMTP-Server mit aufgelistet sein. |
| Add Relaying for | Dieses Feld dient der Eingabe weiterer Relay Adressen beziehungsweise Subnetzen.<br>Nach dem Speichern werden jeweils weitere Eingabefelder eingeblendet. |

**Sektion Antispam**

**Hinweis:**
Die Antispam Optionen sind erst nach Erwerb des optionalen Protection Packs (VSPP) verfügbar.

| Parameter | Beschreibung |
|---|---|
| **Recommended Settings** | |
| **Use Greylisting** | Aktiviert das **Greylisting** auf dem SEPPmail-System.<br>Durch diese Funktion werden eingehende externe E-Mails - d.h. E-Mails welche von keiner unter **Relaying** eingetragener IP oder Subnetz kommen - nicht mehr unmittelbar sondern zeitlich verzögert angenommen. Dies bewirkt, dass von SPAM-Versendern verwendete Methoden zur direkten Übertragung von E-Mails erfolglos bleiben.<br><br>Der Empfang von gewünschten E-Mails wird durch diese Funktion nicht verhindert, sondern lediglich zeitlich verzögert. Der E-Mail-Server des Absenders wird nach einer kurzen Zeit einen erneuten Zustellversuch unternehmen. Die E-Mail wird dann angenommen.<br> <br>**Hinweis:**<br>Diese Funktion ist nur wirksam, wenn das SEPPmail-System eingehende E-Mails direkt dem Internet direkt empfängt (Einstellung **Outgoing Server** **Use built-in mail transport agent**). Bereits von einem anderen E-Mail-Server empfangene und weitergeleitete SPAM E-Mails können durch diese Funktion nicht vermieden werden |

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| | **Hinweis zum Greylisting**<br>Greylisting ist eine Methode zur Bekämpfung von SPAM E-Mails. Bei dieser Funktion wird davon ausgegangen, dass E-Mail-Server und E-Mail-Clients sich an den RFC-Standard für SMTP halten. SPAM-Versender halten sich meist nicht an den RFC-Standard. Sie werten in der Regel das temporäre Abweisen nicht aus, wodurch eine weiterer Zustellversuch unterbleibt.<br>Da sich selbst per E-Mail verbreitende Viren - sogenannte Würmer - nach dem Gleichen Prinzip arbeiten, bietet Greylisting auch hier entsprechenden Schutz.<br><br>Um eventuelle Einschränkungen durch übermässiges, einmaliges Abweisen gewünschter E-Mails zu vermeiden, wird empfohlen die Option **Greylist learning only (no mail rejection)** aus den **"optional Settings"** für zwei bis vier Wochen zu aktivieren. Hierdurch wird die SEPPmail Appliance bezüglich des Greylistings in einem Lernmodus und weist keine E-Mails temporär zurück. |
| **Use Antispam Engine (Note: remember to activate in ruleset)** | Dieser Parameter aktiviert den SPAM-Filter auf dem SEPPmail-System. Die Konfiguration des SPAM-Filters wird im **Ruleset Generator** im Menü **Mail Processing** 147 durchgeführt. |
| **Use Antivirus Engine (Note: remember to activate in ruleset)** | Dieser Parameter aktiviert den Virenscanner auf dem SEPPmail System. Die Konfiguration des Virenscanners wird im **Ruleset Generator** im Menü **Mail Processing** 147 durchgeführt. |
| **Require HELO command** | Nach Aktivieren dieses Parameters prüft die SEPPmail, ob das HELO Kommando vom absendenden E-Mail-Server gesendet wurde. Wird das Kommando nicht gesendet, so wird die Entgegennahme der E-Mails verweigert. |
| **PTR check (reverse DNS lookup)** | SPAM-Versender benutzen häufig E-Mail-Server ohne gültigen DNS-Eintrag. Wird diese Option aktiviert, so werden E-Mails von Servern zu deren IP-Adresse keinen gültiger DNS-Eintrag vorhanden ist abgewiesen. |
| **Check if sender domain is valid** | Mit dieser Option wird das Überprüfen der Absender Domäne (der Teil hinter dem @ der absendenden E-Mail-Adresse) eingehender E-Mails aktiviert. Wird diese nicht per DNS aufgelöst werden, so wird die E-Mail abgewiesen. |
| **Require valid hostname in HELO command** | Ist diese Option aktiviert, so werden nur E-Mails von Servern angenommen, welche sich im HELO Kommando mit einem gültigen - das heisst im DNS auflösbaren - Hostnamen melden. Dies könnte auch ein NetBIOS Name sein. |
| **Require fully qualified hostname in HELO command** | Durch Aktivieren dieser Option werden nur E-Mails von Servern angenommen, welche sich im HELO Kommando mit ihrem vollständigen, im DNS auflösbaren FQDN (Fully qualified domain name) identifizieren. Der FQDN erforder midestens eine Punkt ".", also zum Beispiel "seppmail.ch". |
| **Limit incoming connections for SMTP per IP** | Mit dieser Einstellung werden die parallelen Verbindungen über den TCP Port 25 auf maximal zehn pro IP-Adresse limitiert. Hierdurch kann das Überlasten der SEPPmail-Appliance durch einzelne Server vermieden werden. |
| **optional Settings** | |

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| **Greylist learning only (no mail rejection)** | Dieser Parameter aktiviert den Greylisting-Lernmodus. Dabei wird die Datenbank mit den für den Greylisting-Betrieb benötigten Informationen aufgebaut. Bei Neuinstallationen wird empfohlen diese Option zwei bis vier Wochen zu verwenden, um in der Statrphase keine Engpässe durch das Greylisting zu verursachen. |
| **Strict PTR check (reserse DNS lookup)** | Diese Option aktiviert eine doppelte DNS Prüfung. Zunächst wird geprüft, ob zur IP-Adresse ein gültiger DNS Eintrag vorhanden ist um im Anschluss zu prüfen, ob die DNS-Abfrage die ursprüngliche IP ausgibt. |

**Sektion Blacklists**

| Parameter | Beschreibung |
|---|---|
| **Add Blacklist (RBL)** | E-Mail-Server werden aufgrund von SPAM-Aktivitäten in sogenannte Blacklists aufgenommen. Diese Listen werden durch verschiedene Anbieter im Internet gepflegt. Um E-Mails von Servern welche in diesen Listen aufgeführt sind abzuweisen, müssen die URLs der gewünschten Realtime Blackhole Lists (RBL) eingetragen werden.<br>Nach dem Speichern wird jeweils ein weiteres Eingabefeld eingeblendet. |

**Sektion Manual Blacklisting / Whitelisting**

In diesem Menüpunkt kann der Empfang von externen E-Mails von bestimmten IP-Adressen beziehungsweise -Netzwerken blockiert oder explizit zugelassen werden.

<table>
<tr><th>Parameter</th><th>Beschreibung</th></tr>
<tr><td>add acccess entry</td><td>Für das Blockieren oder Zulassen wird das IP-Netzwerk, die Aktion und einen Kommentar in die entsprechende Eingabefelder eingetragen.
<table>
<tr><th>network:</th><th colspan="2">action:</th><th>comment:</th></tr>
<tr><td rowspan="2">IP-Adresse oder Netzwerk in der angegebenen Form</td><td>accept</td><td>aktzeptiert die Annahme (Whitelist)</td><td rowspan="2">Aussagekräftiger Kommentar, weshalb die Regel eingetragen wurden und wen diese betrifft.</td></tr>
<tr><td>reject</td><td>verweigert die Annahme (Blacklist)</td></tr>
</table>
Beispiel:<br>Um alle E-Mails die aus dem IP-Netzwerk Bereich 186.56.148.x gesendet werden zu verwerfen, geben Sie den IP-Netzwerk Teil 186.56.148 ein und definieren Sie die Aktion reject.</td></tr>
</table>

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| | network: / action: / comment:<br>**186.56.148** / **reject** / Diese Testregel weist alle E-Mails ab, welche aus dem IP-Adressbereich 186.56.148.0 /24 kommen. |

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

### 7.5.1 Untermenü Add/Edit Managed Domain

**Sektion Settings**

Bei der Anlage einer neuen Managed Domain über die Schaltfläche **Add Managed Domain...** ist nur diese Sektion zu sehen.

| Parameter | Beschreibung |
|---|---|
| **Domain Name** | Name der E-Mail Domäne, für welche durch das SEPPmail-System E-Mails angenommen und verarbeitet werden sollen. Es können mehrere E-Mail-Domänen gleichzeitig eingetragen werden. Diese müssen durch Leerzeichen getrennt werden. Die Appliance wird dadurch pro E-Mail-Domäne eine "Managed Domain" mit identischen Einstellungen anlegen.<br><br>Diese Einstellung ist nur beim Anlegen einer neuen "Managed Domain" - das heisst wenn das Menü über die Schalttfläche **Add Managed Domain...** aufgerufen wurde - editierbar.<br><br>**Hinweis:**<br>Werden Subdomänen verwendet, so müssen dies separat aufgeführt werden, damit E-Mail für diese angenommen werden. So werden beispielsweise durch den Eintrag "meinefirma.ch" keine E-Mails für die Subdomäne "tochter.meinefirma.ch" angenommen. |
| **Forwarding Server IP or MX name** | Angabe des E-Mail Servers, an welchen die für den oben genannten **Domain Name** eingehenden E-Mails nach Verarbeitung durch das SEPPmail-System weitergeleitet werden sollen.<br><br>Als Eingabe wird folgendes aktzeptiert:<br><br>IP-Adresse — einzelne IP-Adresse (in eckige Klammern [ ] zu setzen).<br><br>Hostname — wird ein Hostname verwendet, so ist dieser in eckige Klammern [ ] zu setzen. Namen ohne Klammern werden als MX-Eintrag behandelt<br><br>MX-Name — MX-lookup wird ausgeführt<br><br>Optional ist bei Angabe einer IP-Adresse oder eines Hostnamens zusätzlich die Angabe eines individuellen Ports möglich. Dieser wird direkt im Anschluss mit einem Doppelpunkt ":" getrennt angegeben, also "IP-Adresse:Port" oder "Hostname:Port". Wird kein Port angegeben, so wird der Standard SMTP-Port TCP25 verwendet. |

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| **Assigned to Customer** (nur bei Mandanten-fähigen Systemen) | Zuordnung zu einem unter **Customers** bereits angelegten Kunden in einem mandantenfähigem System.<br><br>Die Zuordnung zu einem Kunden ist nur beim Anlegen einer neuen Managed Domain - das heisst wenn das Menü über die Schalttfläche **Add Managed Domain...** aufgerufen wurde - möglich. |

**Hinweis:**
Alle folgenden Einstellungen sind nur zu sehen, wenn das Menü durch Klicken auf eine "Managed Domain" aus dem übergeordneten Menü aufgerufen wurde.

**Sektion External Authentication**

Wird die GINA-Technologie auch intern eingesetzt, zum Beispiel für das Large File Management (LFM) oder Internal Mail Encryption (IME), so ermöglicht diese Option die Authentisierung der Benutzer der "jeweiligen Managed Domain" gegen einen "externen" LDAP-Server (zum Beispiel Active Directory).

| Parameter | Beschreibung |
|---|---|
| **Authenticate GINA users from this domain to external LDAP server (eg. Active Directory)** | Mit Anwahl dieser Option wird die "externe" LDAP Authentisierung" aktiviert. |
| Server | Angabe des LDAP Servers, gegen welchen authentisiert werden soll. Als Eingabe wird der Hostname oder die IP-Adresse aktzeptiert. |
| Port | Gibt den Port an, auf welchem der externe LDAP-Server Anfragen entgegen nimmt. Standard LDAP-Port ist 389, beziehungsweise 636 für LDAPS (siehe auch TLS required). |
| TLS required | Wird diese Option aktiviert, so wird das Verschlüsseln der Verbindung zum LDAP-Server mittels TLSv1 oder höher erzwungen (LDAPS oder LDAPS+STARTTLS). |
| Bind DN | Eingabe des vollständigen Distinguished Name (DN) des read-only Accounts, welcher zur Suche des unter "**External User Attributes** Search Base E-Mail Attribute" in der LDAP Datenbank berechtigt ist. |
| Bind Password | Passwort für das authentisieren des unter Bind DN einegebenen Accounts. |
| **External User Attributes** | <table><tr><td>LDAP ObjectClass</td><td>Eingabe der LDAP-Klasse der Benutzerobjekte am externen LDAP-Server. Standard ist "*"</td></tr><tr><td>Search Base</td><td>Suchpfad: Gibt den Zweig der LDAP Datenbank an, in welchem die zu authentisierenden Benutzer</td></tr></table> |

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| | gesucht werden sollen. |
| | E-Mail Attribute (Default: "mail") — Angabe des Attributes der LDAP Datenbank, unter welchem die E-Mail-Adresse des zu authentisierenden Benutzers in der angegebenen Search Base gespeichert ist. Standard ist "mail". |

Funktionsweise:
Wird aufgrund oben genannter Konfiguration die E-Mail Adresse des sich anmeldenden Benutzers (GINA-Accounts) und somit dessen DN in der LDAP Datenbank gefunden, so wird mit dieser DN und dem vom Benutzer im GINA-Interface eingegebenen Passwort ein neuerlicher Bind versucht. Ist dieser Bind erfolgreich, so gilt die Authentifizierung am GINA-Interface ebenfalls als erfolgreich.

Interaktion mit lokalen GINA-Accounts:
Die Accounts müssen weiterhin auf der SEPPmail-Appliance angelegt werden. Ebenso muss ein lokales Passwort gesetzt werden. Dieses Passwort wird jedoch nicht für die Authentisierung verwendet, solange die externe Authentisierung aktiviert ist.
Während der Erstregistrierung des Accounts wird ein entsprechender Hinweis angezeigt.

Die SEPPmail-Appliance führt einen eigenen Zähler für falsche Passwort-Eingaben. Schlägt eine externe Authentisierung öfter fehl als maximal zugelassen, wird der Account lokal temporär deaktiviert. Dabei findet keine Interaktion mehr mit dem externen Server statt, die Deaktivierung ist also ausschliesslich lokal. Somit kann ein SEPPmail-Administrator einen deaktivierten GINA-Account in der SEPPmail-Administrationsoberfläche jederzeit wieder aktiveren oder dauerhaft deaktivieren. Weiterhin besteht die Möglichkeit einzelne GINA-Accounts von der externen Authentisierung auszunehmen. In diesem Fall wird jeweils wieder das lokale Passwort für das Login verwendet. (siehe auch GINA-Benutzer-Details 211 User Data **External Authentication**)

### Sektion openPGP Domain Encryption

In dieser Sektion werden die openPGP Domänen-Schlüssel angezeigt, sofern vorhanden.

| Key ID | User ID | Issued on | Expires on |
|---|---|---|---|
| Zeigt die Key ID des/der openPGP-Domänen-Key(s) an | Zeigt die zur Key ID zugehörige User ID an. Wurde der Key durch die Appliance generiert, so lautet er in der Regel openPGP Domain Encryption <domain-confidentiality-authority@**ihredomain**.ch> | Ausstelldatum des Keys TT-MM-JJJJ | Ablaufdatum des Keys TT-MM-JJJJ |

Durch Klicken der **Key ID** wird ein Untermenü mit Details zum Key geöffnet. Dieses bietet die Möglichkeit den öffentlichen Schlüssel herunterzuladen beziehungsweise das Schlüsselpaar zu löschen.

Über die Schaltfläche **Import openPGP key...** kann ein bereits vorhandenes Schlüsselpaar importiert werden (siehe Untermenü Import openPGP Key 141).

Über die Schaltfläche **Generate new openPGP key** wird ein neues Schlüsselpaar auf der Appliance generiert (siehe Untermenü Import S/MIME Key 142). Die Laufzeit sowie das automatische Aktualisieren des so erzeugten Schlüssels entspricht der unter **CA** internal CA Settings Validity in days (siehe Menü CA 185) eingegebenen.

© 2015 SEPPmail AG

**Sektion S/MIME Domain Encryption**

In dieser Sektion werden die S/MIME Domänen-Schlüssel angezeigt, sofern vorhanden.

| Fingerprint | Issued on | Expires on |
|---|---|---|
| Zeigt den/die Fingerprint/s des/der S/MIME-Domänen-Keys an.<br><br>Ist im übergeordneten Menü **Mail System** **Managed Domains** die Option **Automatically create and publish S/MIME domain keys for all domains** aktiviert, so ist hier mindestens ein Zertifikat zu sehen. | Ausstelldatum des Keys TT-MM-JJJJ | Ablaufdatum des Keys TT-MM-JJJJ |

Durch Klicken des **Fingerprint**s wird ein Untermenü mit Details zum Key geöffnet. Dieses bietet die Möglichkeit den öffentlichen Schlüssel (Zertifikat) herunterzuladen beziehungsweise das Schlüsselpaar zu löschen.

Über die Schaltfläche **Import S/MIME key...** kann ein bereits vorhandenes Schlüsselpaar importiert werden.
Der Schlüsselaustausch zwischen SEPPmail-Systemen erfolgt bei aktivierter Option **Automatically create and publish S/MIME domain keys for all domains** über den "Managed Domain Service" automatisch. Somit wird sichergestellt, dass alle SEPPmail-System untereinander Domänen verschlüsselt kommunizieren.

Über die Schaltfläche **Generate S/MIME key** wird durch die integrierte CA ein neues Schlüsselpaar auf der Appliance generiert. Die Laufzeit für die so generierten Zertifikate beträgt immer zehn Jahre.

**Sektion GINA and Disclaimer Settings**

Über die Auswahl Use GINA Settings können die für die angegebenen E-Mail-Domäne zu verwendenden GINA-Einstellungen ausgewählt werden. Diese können über das Menü **Mail Processing** **GINA Domains** erzeugt und editiert werden.
Bei mandantenfähigen Systemen muss hier zwingend die für den Kunden eigens einzurichtende GINA ausgewählt werden.

Durch die Auswahl Use Disclaimer lässt sich eine Fussnote für ausgehende E-Mails wählen. Fussnoten können über das Menü **Mail Processing** **Edit Disclaimer** erzeugt und editiert werden.

Diese Einstellungen kommen nur dann zum Tragen, wenn die Funktionen im **Ruleset Generator** des Menüs **Mail Processing** aktiviert wurden.

**Sektion TLS settings** (optional)

Soll zum nachgelagerten Groupware System (siehe **Forwarding Server**) eine TLS verschlüsselte Verbindung aufgebaut werden, so kann die TLS Verschlüsselung an dieser Stelle konfiguriert werden.

© 2015 SEPPmail AG

| TLS-Einstellung | Beschreibung |
|---|---|
| **None** | Keine TLS-Verschlüsselung. |
| **May** | E-Mails werden über einen TLS-verschlüsselten Kanal versendet, falls der empfangende E-Mail-Server TLS-Verschlüsselung unterstützt. |
| **Encrypt** | E-Mails werden nur versendet, falls der Versand mittels TLS-Verschlüsselung möglich ist. |
| **Verify** | E-Mails werden nur versendet, falls der Versand via TLS-Verschlüsselung möglich, und das SSL-Zertifikat des empfangenden E-Mail-Servers gültig ist. |
| **Secure** | E-Mails werden nur versendet, falls der Versand via TLS-Verschlüsselung möglich, das SSL-Zertifikat des empfangenden E-Mail-Servers gültig ist und der Name des E-Mail-Servers gemäss Zertifikat erfolgreich überprüft werden kann.<br> Diese Prüfung kann kann nicht bei der Verwendung von Wildcard-SSL-Zertifikaten eingesetzt werden. Hier sollte alternativ die TLS-Einstellung **Fingerprint** verwendet werden. Wird beim Versenden einer E-Mail via TLS-Transportverschlüsselung die Logmeldung ...status=deferred (Server certificate not verified) ausgegeben, so ist Sie das SSL-Zertifikat des empfangenden E-Mail-Servers auf die Verwendung eines Wildcard-Zertifikats zu überprüfen. |
| **Fingerprint** | E-Mails werden nur versendet, falls der Versand via TLS-Verschlüsselung möglich ist und das SSL-Zertifikat des empfangenden E-Mail-Servers dem definierten Fingerprint entspricht. |

**Hinweis:**
Wird hier keine Konfiguration vorgenommen, so gilt die Einstellung "may", das heisst unterstützt das nachgelagerten Groupware System TLS, so wird die SEPPmail-Appliance eine TLS-verschlüsselte Verbindung dort hin aufbauen.
**Für die TLS Verschlüsselung wird das unter SSL eingebundene Zertifikat verwendet**.

Vergleiche auch Untermenü Add TLS Domain 143 Sektion TLS Settings.

### Sektion Domain Statistics

In dieser Statistik werden nur diejenigen Kryptographie-Technologieen angezeigt, welche auf der SEPPmail-Appliance bereits zum Einsatz kamen.

| Parameter | Beschreibung |
|---|---|
| **Number of accounts in this domain** | Anzahl der auf der SEPPmail-Appliance angelegten Benutzer (entspricht User-Lizenzen) |
| **GINA encrypted mails sent** | Anzahl der versendeten E-Mails, welche mittels GINA-Technologie verschlüsselt wurden |

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| **openPGP encrypted mails sent** | Anzahl der versendeten E-Mails, welche mittels openPGP-Technologie verschlüsselt wurden |
| **openPGP encrypted mails received** | Anzahl der empfangenen E-Mails, welche mittels -Technologie verschlüsselt waren |
| **S/MIME encrypted mails sent** | Anzahl der versendeten E-Mails, welche mittels S/MIME-Technologie verschlüsselt wurden |
| **S/MIME encrypted mails received** | Anzahl der empfangenen E-Mails, welche mittels S/MIME-Technologie verschlüsselt waren |
| **S/MIME signed mails sent** | Anzahl der versendeten E-Mails, welche mittels S/MIME-Technologie signiert wurden |
| **S/MIME signed mails received** | Anzahl der empfangenen E-Mails, welche mittels S/MIME-Technologie signiert waren |
| **openPGP Domain encrypted mails sent** | Anzahl der versendeten E-Mails, welche mittels openPGP-Technologie domänenverschlüsselt wurden |
| **openPGP Domain encrypted mails received** | Anzahl der empfangenen E-Mails, welche mittels openPGP-Technologie domänenverschlüsselt waren |
| **S/MIME Domain encrypted mails sent** | Anzahl der versendeten E-Mails, welche mittels S/MIME-Technologie domänenverschlüsselt wurden |
| **S/MIME Domain encrypted mails received** | Anzahl der empfangenen E-Mails, welche mittels S/MIME-Technologie domänenverschlüsselt waren |

Alle vorgenommenen Änderungen werden über die Schaltfläche **Save changes** gespeichert.
Das Löschen einer Domain erfolgt über **Delete Domain**.

**Hinweis:**
Ist einer Domäne gültiges Schlüsselmaterial zugeordnet, so muss dieses vor dem Löschen der Domäne zurückgewiesen (revoked) werden. Andernfalls erscheinen zunächst entsprechende Warnmeldungen.

#### 7.5.1.1 Untermenü Import openPGP Key

**Sektion Key Data**

| Parameter | Beschreibung |
|---|---|
| Passphrase | Eingabe für die Passphrase mit welcher der private openPGP Schlüssel bei Export verschlüsselt wurde. |

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| **Key File** | Über die Schaltfläche "Datei auswählen" wird die openPGP Schlüsseldatei ausgewählt, welche importiert werden soll. Diese muss das komplette Schlüsselpaar, also privaten und öffentlichen Schlüssel enthalten. |
| or Key as string | Alternativ zur Auswahl einer Schlüssel Datei kann der Schlüssel als Text in dieses Feld kopiert werden |

Über die Schaltfläche **Import** wird der Vorgang abgeschlossen.

#### 7.5.1.2 Untermenü Import S/MIME Key

**Sektion Certificate Data**

| Parameter | Beschreibung |
|---|---|
| **Passphrase** | Eingabe für die Passphrase mit welcher der private S/MIME Schlüssel bei Export in eine PKCS#12 Datei verschlüsselt wurde. |
| **PKCS#12 File** | Über die Schaltfläche "Datei auswählen" wird die S/MIME Schlüsseldatei ausgewählt, welche importiert werden soll. Diese muss das komplette Schlüsselpaar, also privaten und öffentlichen Schlüssel enthalten.<br>PKCS#12 Dateien haben die Dateiendung .p12 oder auch .pfx. |

Über die Schaltfläche **Import** wird der Vorgang abgeschlossen.

© 2015 SEPPmail AG

### 7.5.2 Untermenü Add TLS Domain

**Sektion Domain Info**

| Parameter | Beschreibung |
|---|---|
| **Domain Name** | In der Regel wird hier der Name der E-Mail Domäne des Kommunikationspartners eingetragen.<br>Diese Einstellung ist nur beim Anlegen einer neuen TLS-Verbindung - das heisst wenn das Menü über die Schalttfläche **Add TLS Domain...** aufgerufen wurde - editierbar. |
| **Optional Forwarding Server Address** | Wird an dieser Stelle kein Eintrag vorgenommen, so wird der unter "Domain Name" angegebene Name per MX aufgelöst.<br><br>Als Eingabe wird folgendes aktzeptiert:<br><br>IP-Adresse — einzelne IP-Adresse<br><br>Hostname — wird ein Hostname verwendet, so ist dieser in eckige Klammern [ ] zu setzen. Namen ohne Klammern werden als MX-Eintrag behandelt<br><br>MX-Name — MX-lookup wird ausgeführt<br><br>Optional ist bei Angabe einer IP-Adresse oder eines Hostnamens zusätzlich die Angabe eines individuellen Ports möglich. Dieser wird direkt im Anschluss mit einem Doppelpunkt ":" getrennt angegeben, also "IP-Adresse:Port" oder "Hostname:Port". Wird kein Port angegeben, so wird der Standard SMTP-Port TCP25 verwendet. |

**Sektion TLS Settings**

An dieser Stelle wird der Grad der Prüfungen für eine TLS-Verbindung eingestellt:

© 2015 SEPPmail AG

| TLS-Einstellung | Beschreibung |
|---|---|
| **None** | Keine TLS-Verschlüsselung. |
| **May** | E-Mails werden über einen TLS-verschlüsselten Kanal versendet, falls der empfangende E-Mail-Server TLS-Verschlüsselung unterstützt. |
| **Encrypt** | E-Mails werden nur versendet, falls der Versand mittels TLS-Verschlüsselung möglich ist. |
| **Verify** | E-Mails werden nur versendet, falls der Versand via TLS-Verschlüsselung möglich, und das SSL-Zertifikat des empfangenden E-Mail-Servers gültig ist. |
| **Secure** | E-Mails werden nur versendet, falls der Versand via TLS-Verschlüsselung möglich, das SSL-Zertifikat des empfangenden E-Mail-Servers gültig ist und der Name des E-Mail-Servers gemäss Zertifikat erfolgreich überprüft werden kann.<br> <br>Diese Prüfung kann kann nicht bei der Verwendung von Wildcard-SSL-Zertifikaten eingesetzt werden. Hier sollte alternativ die TLS-Einstellung **Fingerprint** verwendet werden.<br>Wird beim Versenden einer E-Mail via TLS-Transportverschlüsselung die Logmeldung ...status=deferred (Server certificate not verified) ausgegeben, so ist Sie das SSL-Zertifikat des empfangenden E-Mail-Servers auf die Verwendung eines Wildcard-Zertifikats zu überprüfen. |
| **Fingerprint** | E-Mails werden nur versendet, falls der Versand via TLS-Verschlüsselung möglich ist und das SSL-Zertifikat des empfangenden E-Mail-Servers dem definierten Fingerprint entspricht. |

**Hinweis:**
Wird hier keine Konfiguration vorgenommen, so gilt die Einstellung "may", das heisst unterstützt das nachgelagerten Groupware System TLS, so wird die SEPPmail-Appliance eine TLS-verschlüsselte Verbindung dort hin aufbauen.
**Für die TLS Verschlüsselung wird das unter SSL eingebundene Zertifikat verwendet**.

Die vorgenommenen Änderungen werden über die Schaltfläche **Save changes** gespeichert.

## Erklärende Anmerkungen:

### Überprüfen des empfangenden E-Mail-Servers auf die Verwendung eines Wildcard-SSL-Zertifikats

Ob ein E-Mail-Server ein Wildcard-SSL-Zertifikat verwendet kann sehr einfach mit dem Kommandozeilentool **OpenSSL** durchgeführt werden.

**Beispiel:**

```
# openssl s_client -starttls smtp -crlf -connect xxx.xxx.xxx.xxx:25
```

Im Beispiel steht xxx.xxx.xxx.xxx für die tatsächliche IP-Adresse des Zielservers. Alternativ kann der Hostname des Zielservers verwendet werden.

© 2015 SEPPmail AG

```
# openssl s_client -starttls smtp -crlf -connect postini.com.s8a1.psmtp.com:25
```

Das Ergebnis der Abfrage wird wie unten dargestellt aussehen. Anhand des Zertifikats-Subject im Parameter **CN** kann festgestellt werden, ob es sich um ein Wildcard-SSL-Zertifikat handelt. Im Beispiel wurde in der Antwort der Wert **CN=*.psmtp.com** zurückgegeben. Somit handelt es sich um ein Wildcard-Zertifikat "*", welches für alle Hosts der Domain **psmtp.com** verwendet werden kann. Ebenfalls interessant ist der **Parameter X509v3 Subject Alternative Name:**. Als Wert wird hier **DNS: *.psmtp.com** zurückgegeben. In diesem Feld können noch weitere Domains enthalten sein.

```
# openssl s_client -starttls smtp -crlf -connect postini.com.s8a1.psmtp.com:25
| openssl x509 -text -noout

  depth=1 C = US, O = Google Inc, CN = Google Internet Authority
  .
  .
  Certificate:
          .
          .
        Subject: C=US, ST=California, L=Mountain View, O=Google Inc, CN=*.
psmtp.com
          .
          .
          .
                    X509v3 Subject Alternative Name:
                DNS:*.psmtp.com
```

Die Darstellung der Ausgabe wurde auf die wesentlichen Informationen reduziert.

## Auslesen des SHA1-Fingerprint aus dem SSL-Zertifikat des empfangenden E-Mail-Servers

Einen Schritt zuvor wurde beschrieben, wie das vom empfangenden E-Mail-Server verwendete SSL-Zertifikat ausgelesen werden kann. Dabei ist es nicht relevant, ob es sich hierbei um ein Wildcard-Zertifikat handelt oder nicht.

Der Fingerprint eines SSL-Zertifikats kann relativ einfach mir dem Kommandozeilentool **OpenSSL** ausgelesen werden.

**Beispiel:**

```
# openssl s_client -starttls smtp -crlf -connect xxx.xxx.xxx.xxx:25 | openssl
x509 -noout -fingerprint
```

Auch in diesem Beispiel steht xxx.xxx.xxx.xxx für die tatsächliche IP-Adresse des Zielservers, welche alternativ durch den Hostnamen des Zielservers ersetzt werden kann.

```
# openssl s_client -starttls smtp -crlf -connect postini.com.s8a1.psmtp.com:25
| openssl x509 -noout -fingerprint
```

Die daraus resultierende Ausgabe sollte wie folgt aussehen:

```
# openssl s_client -starttls smtp -crlf -connect postini.com.s8a1.psmtp.com:25
| openssl x509 -noout -fingerprint

depth=1 C = US, O = Google Inc, CN = Google Internet Authority
```

© 2015 SEPPmail AG

```
verify error:num=20:unable to get local issuer certificate
verify return:0
250 HELP
SHA1 Fingerprint=DD:9A:EC:66:E2:43:81:B9:20:2B:75:DB:30:C8:67:CC:9B:B0:D1:99
read:errno=0
```

In der Ausgabe wird der benötigte SHA1 Fingerprint angezeigt. Dieser Wert kann nun in die Konfiguration übernommen werden.

© 2015 SEPPmail AG

## 7.6 MailProcessing

Im Menüpunkt **Mail Processing** wird das Regelwerk des SEPPmail-Systems konfiguriert. Dieses Regelwerk ist mit einem Workflow System vergleichbar und stellt das zentrale Element der SEPPmail-Appliance dar.

### Sektion GINA Domains

Indiviuduelle Einstellungen zu den einzelnen GINA-Interfaces.

| Parameter | Beschreibung |
|---|---|
| **Auswahl der zu bearbeitenden GINA Domain** | Im Standard ist an dieser Stelle eine "[default]" GINA vorhanden. Sollte nur ein GINA Webinterface benötigt werden, so ist es ausreichend diese "[default]" Einstellungen individuell anzupassen.<br>Sollten mehrere "Managed Domains" auf dem System eingerichtet sein, so können über die Schaltfläche **Create new GINA domain** weitere GINA Webinterfaces eingerichtet werden (siehe Untermenü Create new GINA Domain 164). Bei einer mandantenfähigen Installation ist es zwingend erforderlich, für jeden Kunden wenigstens eine GINA Webinterface zu erstellen.<br>Das Einrichten erfolgt jeweils durch Auswahl der zu konfigurierenden GINA über das Drop-Down-Menü und klicken der Schaltfläche **Edit**. (siehe Untermenü Untermenü GINA Settings 165).<br><br>Die Zuordung des jeweiligen GINA Webinterfaces zur jeweiligen "Managed Domain" erfolgt in der **Sektion** GINA and Disclaimer Settings des Untermenüs Add/Edit Managed Domain 136 aus **Mail System** Managed Domains.<br><br>Soll ein GINA Webinterface über die Schaltfläche **Delete** gelöscht werden, so ist vorher unbedingt zu überprüfen, dass dieses keiner Managed Domain zugeordnet ist.<br><br>**Hinweis:**<br>**Die "[default]" GINA muss in jedem Fall konfiguriert werden, da Sie als Basis für gegebenenfalls weitere GINA Interfaces dient.**<br>**Unterbleibt dies, so ist mit sporadischen Fehlern der Appliance zu rechnen!** |

### Sektion GINA Settings

Allgemeine Einstellungen der GINA-Interfaces.

| Parameter | Beschreibung |
|---|---|
| **Password Length** | Die hier angebenene Passwort-Länge bezieht sich auf das Initial-GINA-Passwort, welches von der Appliance generiert wird. Standard ist acht "8" Zeichen.<br>Wird die Passwort-Länge auf null "0" gesetzt, so ist für die initiale GINA-Anmeldung kein Passwort erforderlich. |

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| | **Hinweis:**<br>**Von der Einstellung null "0" wird aus Sicherheitsgründen dringend abgeraten.**<br>**Auch ist ein Wert kleiner acht"8" Zeichen nicht zu empfehlen.** |
| **Use virtual hosting** | Werden mehrere GINA Webinterfaces verwendet, so wird im Standard nur ein FQDN für den Zugriff verwendet. Für jedes GINA-Webinterface wird ein eigener Ordner unterhalb dieses FQDNs angelegt. Dadurch wird auch bei der Verwendung von mehereren GINA Interfaces nur ein SSL Zertifikat (siehe Menüpunkt SSL 179) für den Zugriff aus dem Internet auf die jeweiligen GINA Webinterfaces benötigt.<br>Wird die Option "**Use virtual hosting**" verwendet, so muss für jedes GINA Webinterface ein eigener FQDN verwendet werden. Dies hat zur Folge, dass auch für jedes GINA Webinterface ein eigenes Zertifikat benötigt wird. Das entsprechende Eingabefeld für das individuelle Zertifikat wird in diesem Fall im Untermenü Edit GINA Settings 165 angezeigt. |
| **Secure GINA track access** | Mit dieser Option werden über den eingetragenen Link erweiterte Informationen in einer GINA-Lesebestätigung bereitgestellt. Aktiviert wird diese Funktion durch eintragen der URL für den Zugriff auf die Administrationsoberfläche der Appliance. Dabei muss sichergestellt werden, dass diese URL von jedem internen E-Mail Client erreichbar ist. |
| **Disallow insecure ciphers** | Diese Option ist im Standard deaktiviert, wodurch der Zugriff auf das GINA Webinterface auch mit älteren Clients / Browsern möglich ist (**RC4 aktiv**). Um das Sicherheitpotential der Appliance auszuschöpfen, sollte die Aktion aktiviert werden. |

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

### Sektion GINA password via SMS

Einstellungen für den automatisierten Passwort Versand via SMS

| Parameter | Beschreibung |
|---|---|
| **Disable** | Der GINA-Passwort-Versand via SMS ist deaktiviert |
| **Use cell phone / GSM modem attached to appliance** | Ist eine Hardware Appliance im Einsatz, so kann an einen USB-Anschluss der Appliance ein Mobiltelefon oder GSM-Modem angeschlossen werden, über welches SMS versendet werden können. Auf ausreichenden Empfang des Mobiltelefons / GSM-Modems ist zu achten. |
| **Use Mail to SMS service (configuration below)** | An dieser Stelle werden die Zugangsdaten für den SMS Versand über einen **Mail to SMS** Dienst eingetragen. Dies kann sowohl ein interner Dienst im Netz des Kunden als auch ein externer Dienst im Internet sein. Der Zugang zu diesem Dienst ist zu gewährleisten (siehe Firewall / Router einrichten 63 ). |

© 2015 SEPPmail AG

<table>
<tr><th>Parameter</th><th>Beschreibung</th></tr>
<tr><td></td><td>
<table>
<tr><th colspan="2">Mail to SMS settings</th></tr>
<tr><td>Mail from:</td><td>Angabe des gewünschten Absenders, der in der SMS erscheinen soll, zum Beispiel "Ihre Firma"</td></tr>
<tr><td>Mail address prefix: <PREFIXMobile#>@</td><td>Mobilfunknummer, über welche die SMS versendet werden soll.<br>Diese Daten stellt der Betreiber des Dienstes zur Verfügung.<br><br>Bei der deutschen Telekom wäre das zum Beispiel "017187654321"</td></tr>
<tr><td>Gateway Domain: <Mobile#>@</td><td>Gateway-Domäne für den SMS-Versand.<br>Diese Daten stellt der Betreiber des Dienstes zur<br>Verfügung.<br><br>Bei der deutschen Telekom wäre das zum Beispiel "t-d1.sms.de"</td></tr>
</table>
</td></tr>
<tr><td>Use xml service (configuration below)</td><td>
An dieser Stelle werden die Zugangsdaten für den SMS Versand über einen XML Dienst eingetragen. Dies kann sowohl ein interner Dienst im Netz des Kunden als auch ein externer Dienst im Internet sein. Der Zugang zu diesem Dienst ist zu gewährleisten (siehe Firewall / Router einrichten 63).
<table>
<tr><td>Server address:</td><td>Server Adresse des Dienstanbieters.<br>Diese Daten stellt der Betreiber des Dienstes zur Verfügung.</td></tr>
<tr><td>xml template</td><td>Diese Daten stellt der Betreiber des Dienstes zur Verfügung. EinBeispiel hierfür findet dich unten in diesem Abschnitt</td></tr>
</table>
Weiterhin werden die zur Verfügung stehenden Variablen angezeigt
<table>
<tr><th colspan="2">Placeholders:</th></tr>
<tr><td>$sms: Text message</td><td>zu übermittelnder Nachrichtentext.</td></tr>
<tr><td>$number: cell number including country code (+xx...)</td><td>Mobilfunkrufnummer incl. Landesvorwahl (+xx...)</td></tr>
<tr><td>$countrycode: country code, e. g. "49"</td><td>Landesvorwahl, zum Beispiel "49" für Deutschland</td></tr>
<tr><td>$localnumber: cell number without country code</td><td>Mobilfunkrufnummer OHNE Landesvorwahl</td></tr>
</table>
sowie eine Beispielkonfiguration:
<table>
<tr><th colspan="2">XML Example:</th></tr>
<tr><td>Server:</td><td>https://xml1.aspsms.com</td></tr>
</table>
</td></tr>
</table>

© 2015 SEPPmail AG

<table>
<tr><th colspan="2">Parameter</th><th>Beschreibung</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>String:</td><td><?xml version="1.0" encoding="UTF-8"?><br><aspsms><br><Userkey>xyz</Userkey><br><Password>xyz</Password><br><Originator>Secmail</Originator><br><FlashingSMS>1</FlashingSMS><br><Recipient><br><PhoneNumber>$number</PhoneNumber><br></Recipient><br><MessageData><![CDATA[$sms]]></MessageData><br><Action>SendTextSMS</Action><br></aspsms></td></tr>
</table>
</td></tr>
<tr><td></td><td>Use HTTP GET service (configuration below)</td><td>
An dieser Stelle werden die Zugangsdaten für den SMS Versand Dienst per HTTP Get eingetragen. Dies kann sowohl ein interner Dienst im Netz des Kunden als auch ein externer Dienst im Internet sein. Der Zugang zu diesem Dienst ist zu gewährleisten (siehe Firewall / Router einrichten 63).
<table>
<tr><td>Server address:</td><td>Den Server für den Zugang zum HTTP Get Service stellt SMS-Provider zur Verfügung.</td></tr>
<tr><td>HTTP Get String</td><td>Den String für den Zugang zum HTTP Get Service stellt SMS-Provider zur Verfügung.</td></tr>
</table>
Es stehen die aus der XML-Konfiguration bekannten Variablen zur Verfügung.<br><br>
Weiterhin wird die Beispielkonfiguration für den schweizer Dienst "chrus" angezeigt.
<table>
<tr><th colspan="2">HTTP GET Example:</th></tr>
<tr><td>Server:</td><td>https://www.chrus.ch</td></tr>
<tr><td>String:</td><td>/mysms/http/send.php?user=xyz&pwd=xyz&from=Secmail&to=$number&msg=$sms</td></tr>
</table>
</td></tr>
<tr><td colspan="2">Access to GINA send password form:</td><td>Über diese Option wird der Zugriff auf den Passwort-Versand-Link der Appliance gesteuert.</td></tr>
<tr><td></td><td>Disabled</td><td>Damit wird der Passwort-Versand-Link deaktiviert. Somit erscheint dieser auch nicht in der Passwort-Mail, welche beim initialen Versand einer GINA-Mail an den Absender der E-Mail gesendet wird.</td></tr>
<tr><td></td><td>Available via public GINA GUI</td><td>Aktiviert das Einfügen des Links für den SMS-Passwortversand in der GINA-Passwort-Benachrichtigungs-E-Mail an den Absender.</td></tr>
</table>

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

**Sektion Edit Disclaimer**

Fussnoten Einstellungen.

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| **Auswahl der zu bearbeitenden Fussnote (Disclaimer)** | Die Verwendung eines Disclaimers ist optional. Sollen Disclaimer verwendet werden, so können vorhandene Disclaimer - nach entsprechender Auswahl über das Drop-Down-Menü - über die Schaltfläche **Edit** (siehe Untermenü **Edit Disclaimer** 178) angepasst oder auch weitere Disclaimer über die Schaltfläche **Create new disclaimer** angelegt werden.<br>Disclaimer stehen immer sowohl im Text- als auch im HTML-Format zur Verfügung. Beim E-Mail-Versand wird das passende Format anhand des E-Mail-Formats automatisch ausgewählt.<br><br>Die Zuordung des jeweiligen Disclaimers zur jeweiligen "Managed Domain" erfolgt in der **Sektion GINA and Disclaimer Settings** des Untermenüs **Add/Edit Managed Domain** 136 aus **Mail System Managed Domains**.<br><br>Soll ein Disclaimer über die Schaltfläche **Delete** gelöscht werden, so ist vorher unbedingt zu überprüfen, dass dieser keiner Managed Domain zugeordnet ist, beziehungsweise gegebenenfalls in **Custom Command**s der Sektion **Ruleset Generator** dieses Menüs verwendet wird.<br><br>**Hinweis:**<br>**Sollen Disclaimer verwendet werden, so ist unbedingt darauf zu achten, dass diese noch auf dem Groupware System oder durch die SEPPmail-Appliance gesetzt werden. Werden Disclaimer bei ausgehenden E-Mails durch ein nachgelagertes System angehängt, so wird bei durch die Appliance S/MIME signierten E-Mails diese Signatur zerstört.** |

**Sektion Edit Mail Templates**

E-Mail-Vorlagen Einstellungen.

| Parameter | Beschreibung |
|---|---|
| **Auswahl der zu bearbeitenden E-Mail Vorlage (Templates) für Bounce-Mails** | E-Mail-Templates sind vordefinierte Nachrichten, welche in definierten Fällen automatisiert versendet werden. Diese Templates können innerhalb eines **Custom Command**s der Sektion **Ruleset Generator** dieses Menüs verwendet werden.<br><br>Im Standard ist lediglich das Template "bounce_noenc" vorhanden. Dieses sowie gegebenenfalls selbst erzeugte Templates können - nach entsprechender Auswahl über das Drop-Down-Menü - über die Schaltfläche **Edit** angepasst werden. Das Anlegen neuer Templates erfolgt über die Schaltfläche **Create new template**.<br>Abhängig von spezifischen Einstellungen des Rulests (siehe **Ruleset Generator**) werden weitere Standard Templates verwendet ("bounce_noseckey", "bounce_noauth") verwendet. Diese sind in der Auswahl nicht zu sehen, können jedoch durch Erstellen mittels **Create new template** ebenfalls angepasst werden. |

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| | **Hinweis:**<br>**Bei der Anlage neuer Templates kann über den Template Namen gesteuert werden, ob die Original-E-Mail als Anhang angefügt wird oder nicht.**<br>**Wird im Template Namen "attachmail" gefunden, so wird die ursprüngliche E-Mail angefügt.**<br><br>Soll ein Template über die Schaltfläche **Delete** gelöscht werden, so ist vorher unbedingt zu überprüfen, dass dieses in **Custom Command**s der Sektion **Ruleset Generator** dieses Menüs verwendet wird. |

**Sektion Miscellaneous Options**

Sonstige Einstellungen.

| Parameter | Beschreibung |
|---|---|
| **automatically send new openPGP public keys to users when a key is created** | Ist der Sektion **Ruleset Generator** dieses Menüs unter "Key Generation" die Option "automatically create openPGP keys for new users" aktiv, so wird durch Aktivieren dieser Option der öffentliche Schlüssel des automatisch generierten Schlüsselpares an den neu erzeugte Benutzer gesendet.<br>Dadurch wird dieser Benutzer in die Lage versetzt, seinen öffentliche Schlüssel selbst an Kommunikationspartner weiterzugeben. Diese werden dadurch wiederum in die Lage versetzt, openPGP verschlüsselt mit diesem Benutzer zu kommunizieren. |

**Hinweis:**
**Dieser Parameter wird nicht im Cluster synchronisiert. Das heisst in einem Cluster Umfeld muss der Parameter auf jedem Cluster Teilnehmer einzeln konfiguriert werden**

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

**Sektion Ruleset Generator**

Mit dem **Ruleset Generator** wird quasi ein "Workflow System" für eingehende und ausgehende E-Mails definiert.

Die in dieser Sektion vorhandenen Eingabefelder für Betreffzeilen-Schlüsselworte (text in subject) sind mit "Regular Expressions" zu befüllen. Das heisst Sonderzeichen müssen mit einem Backslash "\" als solche gekennzeichnet werden. Gruppierungen sind durch Eingrenzen mit runden Klammern "()" vorzunehmen. Eine Aneinanderreihung mehrerer Schlüsselwort ist durch das Trennen mit dem Pipe-Zeichen "|" möglich.
Beispiel:

Soll als Betreffzeilen-Schlüsselwort <abc> verwendet werden so ist diese wie folgt einzugeben: \<abc\>

Soll sowohl das Betreffzeilen-Schlüsselwort <abc> als auch [def] verwendet werden so ist diese wie folgt einzugeben: (\<abc\>)|([def])

Gross-/Kleinschreibung wird bei der Eingabe des Schlüsselwortes in der Betreffzeile ignoriert.
Bei Verwenden des SEPPmail-Outlook-AddIns im Betreffzeilen-Modus ist darauf zu achten, dass bei

© 2015 SEPPmail AG

Änderungen der Schlüsselworte in der Appliance, diese entweder als zusätzliche Werte hinzugefügt werden, oder die Werte im AddIn an die Werte der Appliance angepasst werden müssen.

| Beschreibung | |
|---|---|
| **General Settings** | |
| Do not touch mails with the following text in subject: | Ist diese Option aktiv und das angegebene Schlüsselwort wird im Betreff einer ausgehenden E-Mail gefunden, so wird diese kryptographisch unbehandelt weitergeleitet. Das Ruleset wird nicht weiter durchlaufen.<br>Im Standard lautet das Schlüsselwort \[plain\].<br>Dies ergibt unter Umständen Sinn, wenn all diese Voraussetzungen gegeben sind:<br>• Einstellung "Always use S/MIME or openPGP if keys are available" an der OEM-PRODUCTNAME%>-Appliance aktiv<br>• Absender weiss, dass der Empfänger temporär nur auf einem Mobilen Endgerät empfangen kann<br>• Inhalt der E-Mail ist nicht vertraulich |
| Add disclaimer to all outgoing emails | Mit dem Aktivieren dieser Funktion wird jeder ausgehenden, initialen E-Mail die Fussnote angehängt, welche der jeweiligen Managed Domain (siehe Menü **Add/Edit Managed Domain** 136 **GINA and Disclaimer Settings**) zugeordnet ist. |
| Also add disclaimer to replies (in-reply-to header set) | Durch das Aktivieren dieses Punktes wird nicht nur initialen E-Mails, sondern auch Antwort-E-Mails die jeweils zugeordnete Fussnote angehängt. |
| Reprocess mails sent to reprocess@decrypt.reprocess | Diese Funktion ermöglicht es einem Empfänger eine verschlüsselte E-Mail aus seinem Postfach erneut an die SEPPmail-Appliance zur Entschlüsselung zu senden. Hierfür ist die Verschlüsselte E-Mail als Anhang in eine neue E-Mail zu packen und an die Adresse "reprocess@decrypt.reprocess" zu senden. Die ursprünglich verschlüsselte Nachricht wird dadurch entschlüsselt - natürlich vorausgesetzt der entsprechende Schlüssel ist der OEM-PRODUCTNAME%>-Appliance bekannt - und zurück gesendet.<br>Anwendungsbeispiele könnten sein:<br>• Direktes Weiterleiten verschlüsselter E-Mails an den internen E-Mail Server bei Ausfall der Appliance<br>• Migration von lokalem Schlüsselmaterial auf den Clients hin zur OEM-PRODUCTNAME%>-Lösung bei gleichzeitigen zurückbleiben von verschlüsselten E-Mails in den Postfächern der Empfänger<br>Ebenso ermöglicht dieser Befehl openPGP verschlüsselte Dateien aus dem Datei System durch Senden als E-Mail Anlage an diese Adresse zu entschlüsseln. |
| Show message subject in logs | Zeigt die Betreffzeilen von E-Mails im E-Mail-Log der Appliance an. Dies erleichtert oft die Fehleranalyse. Sollte diese Anzeige jedoch aus revisionstechnischen Gründen untersagt sein, so ist das Ausblenden durch Deaktivieren dieser Option möglich. |
| **User Creation** | |
| Manual user creation: Only process outgoing mails from users with an account | Mit dieser Option können Benutzer auf der Appliance nur manuell angelegt werden. |

© 2015 SEPPmail AG

| Beschreibung | |
|---|---|
| | **Hinweis:**<br>**Wird diese Einstellung gewählt, so ist sicherzustellen, dass kein Absender, welcher in der OEM-PRODUCTNAME%>-Appliance nicht bereits als Benutzer angelegt ist, Merkmale zur kryptographischen Behandlung (Schlüsselwort, AddIn, Header) verwendet.**<br>**In dieser Konstellation würde die Anforderung ignoriert und somit die E-Mail ohne die gewünschte kryprtographische Aktion versendet.**<br>Dieses Verhalten kann bei Bedarf durch einen **Custom Command** dahingehend geändert werden, dass E-Mails in dieser Konstellation abgewiesen werden (siehe **Bounce von E-Mails nicht authentifizierter Benutzern** 301). |
| automatically create accounts for new users if user tries to sign / encrypt | Durch Aktivieren dieser Option wird ein Absender, der über ein entsprechendes Merkmal eine E-Mail als zu verschlüsselnd oder zu signierend markiert automatisch als Benutzer auf der OEM-PRODUCTNAME%>-Appliance angelegt werden, sofern er nicht bereits vorhanden ist.<br>Bei Verwenden dieser Option ist darauf zu achten, dass genügend freie Benutzerlizenen vorhanden sind (siehe **Home** 116 **License Encryption/Signature Licenses**) |
| automatically create accounts for all users | Kreiert für jeden Absender der über die OEM-PRODUCTNAME%>-Appliance eine E-Mail sendet einen Benutzer, egal, ob Verschlüsseln/ Signieren angefordert wurde oder nicht.<br>Diese Einstellung ist geeignet, wenn die OEM-PRODUCTNAME%>-Appliance nicht direkt im E-Mail Strom steht, sondern bereits über eine vorgelagerte Komponente entschieden wird, welche E-Mails kryptographisch zu behandelnd sind und nur diese an die OEM-PRODUCTNAME%>-Appliance übergibt.<br>Ein weiterer Anwendungsfall wäre, wenn alle E-Mails eines Unternehmens grundsätzlich signiert oder gegebenenfalls verschlüsselt werden sollen. |
| **Encryption/Decryption** | |
| Incoming e-mails | |
| Add this text to message subject after decryption | Ist diese Option aktiv, werden eingehende, durch die OEM-PRODUCTNAME%>-Appliance entschlüsselte E-Mails im Betreff mit diesem Schlüsselwort gekennzeichnet.<br>Im Standard lautet das Schlüsselwort \[secure\]. |
| Set confidential flag after decryption: | Durch Aktivieren dieser Option wird bei eingehenden, durch die OEM-PRODUCTNAME%>-Appliance entschlüsselten E-Mails den Header "Sensitivity: Confidential" . |
| Reject mails if S/MIME decryption fails | Bei aktiver Option werden eingehende, verschlüsselte E-Mails abgewiesen (bounced), sofern sie durch die OEM-PRODUCTNAME %>-Appliance nicht entschlüsselt werden konnten.<br>Da die OEM-PRODUCTNAME%>-Appliance eine E-Mail einem eventuell vorgelagerten System erst dann als angenommen meldet, wenn die E-Mail ausgeliefert werden kann, ist diese Funktion auch |

© 2015 SEPPmail AG

| Beschreibung | |
|---|---|
| | zum Beispiel nach einem externen SPAM-Filter problemlos verfügbar.<br> <br>**Hinweis:**<br>**Durch Aktivieren dieser Aktion wird auch eine eventuell teilweise Ende-zu-Ende Verschlüsselung (zum Beispiel mittels Smart-Card) unterbunden.** |
| Outgoing e-mails | |
| Always encrypt mails with the following text in subject: | Ist diese Option aktiv und das angegebene Schlüsselwort wird im Betreff einer ausgehenden E-Mail gefunden, so wird diese verschlüsselt.<br>Im Standard lautet das Schlüsselwort \[confidential\]. |
| Always encrypt mails with Outlook "confidential" flag set | Bei aktiver Option wir der "Sensitivity" Parameter aus dem E-Mail Header der ausgehenden E-Mail ausgewertet. Hat dieser den Wert "confidential", so wird die E-Mail verschlüsselt. |
| Always use GINA technology for mails with the following text in subject: | Ist diese Option aktiv und das angegebene Schlüsselwort wird im Betreff einer ausgehenden E-Mail gefunden, so wird das Verschlüsseln mittels GINA-Technologie erzwungen.<br>Im Standard lautet das Schlüsselwort \[priv\].<br>Das Erzwingen der GINA-Technologie ist immer dann sinnvoll, wenn eine verlässliche Lesebestätigung benötigt wird. |
| Always use GINA technology for mails with Outlook "private" flag set | Bei aktiver Option wir der "Sensitivity" Parameter aus dem E-Mail Header der ausgehenden E-Mail ausgewertet. Hat dieser den Wert "private", so wird ebenfalls das Verschlüsseln mittels GINA-Technologie erzwungen.<br> <br>**Hinweis:**<br>**Diese Option kann zu Problemen führen, wenn als privat markierte Kalendereinträge versendet werden, da diese dann automatisch** GINA-**verschlüsselt würden.** |
| Create GINA users with empty password if the following text is in the subject: | Mit Aktivieren dieses Punktes wird bei Auffinden des angegebenen Schlüsselwortes im Betreff einer ausgehenden, initialen GINA-E-Mail kein Initial-Password benötigt.<br>Im Standard lautet das Schlüsselwort \[emptypw\]. |
| Always use S/MIME or openPGP if keys are available | Bei aktiver Option werden ausgehende E-Mails immer verschlüsselt, sofern der OEM-PRODUCTNAME%>-Appliance ein öffentlicher Schlüssel - egal ob S/MIME oder openPGP - des Kommunikationspartners (Empfängers) vorliegt.<br> <br>**Hinweis:**<br>**Es gilt zu beachten, dass der Versender der E-Mail auf der OEM-PRODUCTNAME%>-Appliance jeweils als Benutzer angelegt sein oder werden muss, wenn er an einen entsprechenden Kommunikationspartner sendet.** |

© 2015 SEPPmail AG

| Beschreibung | |
|---|---|
| | |
| Always use GINA encryption if account exists and no S/MIME or openPGP key is known | Ist diese Option aktiv, so werden ausgehende E-Mails immer mittels GINA-Technologie verschlüsselt, sofern der OEM-PRODUCTNAME %>-Appliance kein öffentlicher Schlüssel - weder S/MIME noch openPGP - bekannt ist, jedoch ein OEM-PRODUCTNAME%>-Account für den Kommunikationspartner (Empfängers) vorliegt. |
| Do not encrypt outgoing mails with the following text in subject: | Ist diese Option aktiv und das angegebene Schlüsselwort wird im Betreff einer ausgehenden E-Mail gefunden, so wird ein eventuelles Verschlüsseln in jedem Fall unterdrückt. Andere kryptographische Aktionen (Signieren) sind davon nicht betroffen.<br>Im Standard lautet das Schlüsselwort \[noenc\]. |
| Use AES256 for S/MIME encryption | Durch das Aktivieren dieser Option wird für das S/MIME Verschlüsseln von E-Mail der AES256 Algorithmus verwendet. Dieser Algorithmus wird von WindowsXP Maschinen sowie in Outlook Versionen vor 2007 nicht unterstützt. |
| **Signing** | |
| Incoming e-mails | |
| Add this text to message subject if S/MIME signature check succeeds: | Ist diese Option aktiv, werden eingehende, signierte E-Mails, deren Signaturen durch die OEM-PRODUCTNAME%>-Appliance geprüft und als in Ordnung befunden wurden mit dem angegebenen Schlüsselwort im Betreff gekennzeichnet.<br>Im Standard lautet das Schlüsselwort \[signed\sok\].<br><br>**Hinweis:**<br>**Damit eine S/MIME E-Mail-Signatur als "in Ordnung" befunden wird,**<br>**a) darf diese E-Mail auf dem Weg vom Absender bis zum Empfang und Prüfung durch die OEM-PRODUCTNAME%>-Appliance nicht veränder worden sein.**<br>**b) muss das Signatur-Zertifikat des Absenders von einem vertrauenswürdigen Aussteller Stammen (siehe X.509 Root Certificates 218)** |
| remove signature if S/MIME signature check succeeds | Entfernt die S/MIME E-Mail-Signatur nach erfolgreicher Prüfung. Das Entfernen der E-Mail-Signatur kann beim Einsatz Mobiler Endgeräte als E-Mail-Clients von Vorteil sein, da diese häufig nicht mit diesen Signaturen umgehen können. |
| Add this text to message subject if S/MIME signature fails: | Ist diese Option aktiv, werden eingehende, signierte E-Mails, deren Signaturen durch die OEM-PRODUCTNAME%>-Appliance geprüft und als defekt befunden wurden mit dem angegebenen Schlüsselwort im Betreff gekennzeichnet.<br>Im Standard lautet das Schlüsselwort \[signed\sINVALID\]. |
| remove signature if S/MIME signature check fails | Entfernt die S/MIME E-Mail-Signatur nach fehlgeschlagener Prüfung. Das Entfernen der E-Mail-Signatur kann beim Einsatz Mobiler Endgeräte als E-Mail-Clients von Vorteil sein, da diese häufig nicht mit diesen Signaturen umgehen können. Allerdings ist dann auch |

© 2015 SEPPmail AG

| Beschreibung | |
|---|---|
| | keine weitere Prüfung durch den E-Mail-Client und somit eine Analyse, weshalb die Signatur als ungültig eingestuft wurde, möglich. |
| Outgoing e-mails | |
| S/MIME sign outgoing mails with domain key with the following text in subject: | Ist diese Option aktiv und das angegebene Schlüsselwort wird im Betreff einer ausgehenden E-Mail gefunden, so wird diese S/MIME signiert.<br>Im Standard lautet das Schlüsselwort \[sign\]. |
| Sign all outgoing e-mails if S/MIME certificate available | Signiert alle ausgehenden E-Mails von OEM-PRODUCTNAME%>-Benutzern mit gültigem S/MIME Zertifikat.<br>Da mit der S/MIME Signatur das öffentliche Zertifikat mitgesendet wird, wird diese durch das Aktivieren dieser Aktion möglichst vielen Kommunikationspartnern zur Verfügung gestellt. Dadurch werden diese widerum in de Lage versetzt S/MIME verschlüsselt mit dem Absender zu kommunizieren.<br>Weiterhin wird hierdurch die Herkunft der E-Mails bestätigt. |
| Do not S/MIME sign outgoing mails with the following text in subject: | Ist diese Option aktiv und das angegebene Schlüsselwort wird im Betreff einer ausgehenden E-Mail gefunden, so wird ein eventuelles Signieren in jedem Fall unterdrückt. Andere kryptographische Aktionen (Verschlüsseln) sind davon nicht betroffen.<br>Im Standard lautet das Schlüsselwort \[nosign\]. |
| S/MIME sign outgoing mails with domain key with the following text in subject: | Ist diese Option aktiv und das angegebene Schlüsselwort wird im Betreff einer ausgehenden E-Mail gefunden, so werden alle ausgehenden E-Mail - egal von welchem Absender - mit dem S/MIME-Zertifikat und im Namen der angegebenen E-Mail-Adresse (siehe "Using Certificate") S/MIME signiert.<br>Im Standard lautet das Schlüsselwort \[domainsign\].<br><br>**Hinweis:**<br>**Vom Verwenden dieser Option wird dringendst abgeraten!**<br>**Durch die für diese Funktion notwendige Manipulation des Absenders aller ausgehenden E-Mails resultieren zahlreiche Probleme.**<br>**So werden sogenannte Non-Delivery-Reports immer an diese Adresse und nicht an den ursprünglichen Absender gesendet. Das heisst kommt eine E-Mail nicht wie erwartet bei Empfänger an, so wird der ursprüngliche Absender darüber keine Information erhalten.**<br>**Trägt der Empfänger den Absender der E-Mail in sein Adressbuch ein, so ist auch hier zu erwarten, dass er zukünftig nicht den eigentlich gewünschten, sondern den manipulierten Empfänger adressiert.** |
| Using Certificate: | Angabe der E-Mail-Adresse wie sie im S/MIME Zertifikat für die Domänensignatur enthalten ist. |
| Text before new FROM: | Einzufügender Text vor dem manipulierten Absender. |
| Text after new FROM: | Einzufügender Text nach dem manipulierten Absender. |

© 2015 SEPPmail AG

| Beschreibung | |
|---|---|
| **Key Generation** | |
| automatically create openPGP keys for new users | Durch Auswählen dieser Option wird für jeden neu generierten Benutzer automatisch ein openPGP-Schlüsselpaar erzeugt. |
| automatically create S/MIME keys for new users | Durch Auswählen dieser Option wird für jeden neu generierten Benutzer automatisch ein S/MIME-Schlüsselpaar über die interne CA erzeugt. |
| automatically buy <CA> S/MIME keys for new users | Durch Auswählen dieser Option wird für jeden neu generierten Benutzer automatisch ein S/MIME-Zertifikat von der angegebenen CA bezogen.<br> <br>**Hinweis:**<br>**Das Schlüsselpaar wird auf der Appliance generiert. Nur der öffentliche Schlüssel wird zum Signieren bei der CA eingereicht. Der private Schlüssel verlässt die OEM-PRODUCTNAME%>-Appliance nicht!**<br>**Diese Option erscheint nur dann, wenn unter CA 185 External CA eine entsprechende MPKI ausgewählt wurde.** |
| **Protection Pack (Anti-Spam / Anti-Virus)**<br>(nur mit entsprechender Lizenz "Anti-spam / Anti-virus" (siehe Home 116 License) verfügbar) | |
| Check mails for viruses and send infected mails to (leave empty to reject infected mails): | Mit Auswahl dieser Option wird der Virenscanner aktiviert. Infizierte E-Mails werden an die optional einzugebende E-Mail-Adresse gesendet (Quarantäne). Bleibt das Eingabefeld für die E-Mail-Adresse leer, so werden infizierte E-Mails abgewiesen (bounced). |
| Send notification to this email address if a virus was found: | Wird an dieser Stelle eine E-Mail-Adresse angegeben, so werden an diese Benachrichtigungen über Virenfunde gesendet. |
| Check incoming mails for spam and add the following text to the subject to identify spam: | Mit Auswahl dieser Option werden als SPAM klassifizierte E-Mails dem angegebenen Text in der Betreffzeile versehen und an den Empfänger weitergeleitet. Basis der Klassifizierung ist der angegebene "Tag level" (siehe nächste Option).<br>Der Standartext für diese Markierung lautet [SPAM]<br>(Achtung: reine Texteingabe, keine "Regular Expression") |
| Tag level: | Auswahl, des Schwellwertes für die SPAM-Erkennung. Je niedriger dieser Wert gesetzt wird, desto strenger sind die Kriterien für die SPAM-Erkennung.<br>Im Standard ist der Wert "5" gewählt.<br>Bei niedrigen Werten erhöht sich das Risiko von Falscherkennungen, so dass legitime E-Mails als SPAM erkannt und markiert werden. |
| Check incoming mails for spam and redirect spam to (leave empty to reject spam): | Mit Auswahl dieser Option werden als SPAM klassifizierte E-Mails an die angegebene Adresse umgeleitet, beziehungsweise bei freilassen des Eingabefeldes abgelehnt (bounced). Basis für die SPAM Erkennung ist der angegebene "Spam level" (siehe nächste Option). |
| Spam level: | Auswahl, des Schwellwertes für die SPAM-Erkennung. Je niedriger dieser Wert gesetzt wird, desto strenger sind die Kriterien für die |

© 2015 SEPPmail AG

| Beschreibung | |
|---|---|
| | SPAM-Erkennung.<br>Im Standard ist der Wert "8" gewählt.<br>Bei niedrigen Werten erhöht sich das Risiko von Falscherkennungen, so dass legitime E-Mails als SPAM erkannt und umgeleitet beziehungsweise abgelehnt (bounced) werden. |
| **Header tagging**<br>Durch das "Header tagging" wird das Setzen eines erweiterten, sogenannten X-Headers und einen zugehörigen Wert für unterschiedliche Situationen (siehe folgende Optionen) durch die OEM-PRODUCTNAME%>-Appliance ermöglicht. Diese erweiterten Informationen können durch nachgelagerte Komponenten ausgewertet werden.<br>Ein Beispiel für so eine zusätzliche, nachgelagerte, E-Mail verarbeitende Komponente könnte ein Data Loss Prevention (DLP) System sein. | |
| Set header  to value  For all incoming mails | Setzt den angegebenen X-Header mit dem zugeordneten Wert für alle eingehenden E-Mails |
| Set header  to value  For all outgoing mails | Setzt den angegebenen X-Header mit dem zugeordneten Wert für alle ausgehenden E-Mails |
| Set header  to value  For all mails that have been encrypted | Setzt den angegebenen X-Header mit dem zugeordneten Wert für alle E-Mails, welche durch die OEM-PRODUCTNAME%>-Appliance verschlüsselt wurden. |
| Set header  to value  For all mails that have been decrypted | Setzt den angegebenen X-Header mit dem zugeordneten Wert für alle E-Mails, welche durch die OEM-PRODUCTNAME%>-Appliance entschlüsselt wurden. |
| **Archiving** | |
| Send a copy of ALL emails to the following Address: | Durch Aktivieren dieser Option wird eine Kopie aller über die OEM-PRODUCTNAME%>-Appliance transportierten E-Mails an die angegebene E-Mail-Adresse gesendet. |
| **Custom Commands**<br>Über Custom Commands können über den in den Regelwerk-Anweisungen 228 definierten Befehlssatz spezifische Anforderungen an entsprechender Stelle im Ruleset eingefügt werden. | |
| Custom commands for incoming e-mails BEFORE decryption: | Fügt bei Aktivierter Option den im Eingabefeld vorhandenen Code an der Stelle im Ruleset für eingehende E-Mails VOR der Entschlüsselung ein. |
| Custom commands for incoming e-mails AFTER decryption: | Fügt bei Aktivierter Option den im Eingabefeld vorhandenen Code an der Stelle im Ruleset für eingehende E-Mails NACH der Entschlüsselung ein. |
| Custom commands for outgoing e-mails BEFORE encryption: | Fügt bei Aktivierter Option den im Eingabefeld vorhandenen Code an der Stelle im Ruleset für ausgehende E-Mails VOR der Verschlüsselung ein. |
| Custom commands for e-mails from GINA: | Fügt bei Aktivierter Option den im Eingabefeld vorhandenen Code an der Stelle im Ruleset für eingehende GINA E-Mails ein. |
| Custom commands for User | Fügt bei Aktivierter Option den im Eingabefeld vorhandenen Code an |

© 2015 SEPPmail AG

| Beschreibung | |
|---|---|
| Creation: | der Stelle im Ruleset für das Generieren neuer Benutzer ein. |

**Key Server**
Über Key Server wird das zusätzliche Abfragen öffentlicher Schlüssel von Kommunikationspartnern für die Verschlüsselung ermöglicht.
Nach dem Speichern eines Key Server Eintrags wird jeweils ein weiteres Eingabefeld eingeblendet.

**Hinweis:**
**Öffentliche Key Server beherbergen häufig "totes" Schlüsselmaterial. Das heisst für die über den Key Server bereitgestellten öffentlichen Schlüssel besitzen die Empfänger oft nicht mehr den privaten Schlüssel. Somit sind diese nicht in der Lage die verschlüsselten E-Mails zu lesen.**
**Aus diesem Grund wird dringend von der Abfrage solcher Server abgeraten.**

| | |
|---|---|
| openPGP Key Server | An dieser Stelle werden Einträge für openPGP Key Server vorgenommen.<br><br>**Hinweis:**<br>**Wird bei der Abfrage eines öffentlichen openPGP Schlüssels ein Schlüssel gefunden, dessen Key ID identisch mit einem bereits vorhandenen Eintrag auf der SEPPmail-Appliance ist, so wird dieser Schlüssel auf der Appliance durch das Ergebnis der LDAP-Abfrage überschrieben.** |
| S/MIME Key Server | An dieser Stelle werden Einträge für S/MIME Key Server vorgenommen. |

**Beispiel Key Server Eintrag:**

| | | | | | |
|---|---|---|---|---|---|
| recipient mask (regexp): | @firma\.ch | URI: | LDAP://ldap.firma.local/ | Bind dn: | CN=MaxMuster, OU=Users, OU=Firma |

| | | | |
|---|---|---|---|
| Bind pw: | password | Base DN: | DC=ihredomain,DC=local |

**Advanced Options**

| | |
|---|---|
| Re-inject mails to sending mailserver | Mit dem Aktivieren dieser Option werden bereits verarbeitete E-Mails an den einliefernden E-Mail-Server zurück gesendet.<br>Forwarding und Outgoing Server werden bei aktivierter Option ignoriert beziehungsweise als Fallback Einstellung verwendet<br><br>**Hinweis:**<br>**Durch das Aktivieren dieser Option kann unter Umständen eine E-Mail Schleife (Loop) erzeugt werden, wenn das einliefernde E-Mail System diese Funktion nicht unterstützt oder falsch konfiguriert wurde.** |
| Run in queueless mode | Schaltet die Warteschlangen Funktion ab. E-Mails werden vom <OEM-PRODUCTNAME%>-System erst dann an das abgebende System als angenommen gemeldet, wenn die E-Mail bereits vom |

© 2015 SEPPmail AG

| Beschreibung | |
|---|---|
| | annehmenden System als angenommen gemeldet wurde.<br>Wird diese Option verwendet, so kann bei einem Austausch der Appliance (zum Beispiel bei einem Hardware-Defekt) sichergestellt werden, dass keine E-Mails verloren gehen. |
| Completely disable GINA technology | Deaktiviert die GINA-Technologie.<br>Als Folge würden als "zu verschlüsselnd" gekennzeichnete E-Mails abgewiesen werden, wenn keine andere Verschlüsselungsmethode (S/MIME, openPGP, Domain) verfügbar ist.<br> **Hinweis:**<br>**Wird die GINA-Technologie über diese Option abgeschaltet, so ist darauf zu achten, dass alle Optionen aus "Encryption/Decryption", welche diese Technologie ansteuern deaktiviert sind. Ebenso darf kein Ansteuern dieser Technologie über "Custom Commands" erfolgen.** |
| Completely disable user-based S/MIME and openPGP | Deaktiviert sowohl die Benutzer bezogene S/MIME als auch die openPGP Technologie.<br>Diese Aktion wird meist in Verbindung mit "Completely disable GINA technology" verwendet, um ausschliesslich Domänen Verschlüsselung anzuwenden.<br> **Hinweis:**<br>**Wird diese Option gewählt, so ist darauf zu achten, dass alle Optionen aus "Encryption/ Decryption", welche diese Technologie ansteuern deaktiviert sind. Ebenso darf kein Ansteuern dieser Technologien über "Custom Commands" erfolgen.** |
| Use remote GINA server, reachable under the following email address: | Muss aus revisionstechnischen Gründen der GINA-Teil in einer anderen Demilitarisierten Zone (DMZ) als der SMTP verarbeitende Teil stehen, so ist die Trennung über diese Option möglich.<br>Alle GINA zu verschlüsselnden E-Mails werden dann über die hier angegebene Pseudo-E-Mail-Adresse (zum Beispiel gina@ginapseudodomain.local) an den GINA-Satelliten geleitet. |
| This is a remote GINA server | Definiert den Gegenpart zur Option "Use remote GINA server, reachable under the following email address:", also den GINA-Satelliten.<br>An der Satelliten-Appliance muss die Pseudo-Mail-Domäne (im Beispiel oben "ginapseudodomain.local") als zusätzliche Managed Domain eingetragen werden (siehe **Mail System** 129 **Managed Domains**). Ebenso müssen die Managed Domains des Basis-Systems erfasst werden. Die GINA-Konfiguration und deren Zuordnung zu den Managed Domains erfolgt auf dem Satelliten-System (siehe **Mail Processing** 147 **GINA domains**). |
| Relay for domain: | Hier sind die "Managed Domains" des "Basis"-Systems einzutragen (siehe **Mail System** 129 **Managed Domains**).<br>Die Trennung der Domains erfolgt durch ein Pipe-Zeichen "\|". |
| Relay email address: | Hier ist die gleiche Pseudo-E-Mail-Adresse einzutragen wie auf dem "Basis"-System unter "Use remote GINA Server, reachable under the |

© 2015 SEPPmail AG

| Beschreibung | |
|---|---|
| | following email address:". |
| Relay domain key fingerprint: | Hier sind die Fingerprints der Domänen Zertifikate der unter "Relay for Domain" angegebenen Managed Domains jeweils durch ein Pipe-Zeichen "\|" getrennt anzugeben.<br>(siehe **Add/Edit Managed Domain** 136 **S/MIME Domain Encryption**) |
| Enable internal encryption with user keys (also enables ldap server on ports 388, 387 and 635. User keys must be installed on appliance for proper function) | Mit dieser Option wird die zertifikatsbasierte interne E-Mail Verschlüsselung aktiviert.<br><br>Im Anschluss müssen die privaten Schlüssel - der vorhandenen unternehmensinternen CA - für die Benutzer, denen das Verschlüsseln zu externen Kommunikationspartnern gestattet ist, auf der %OEM-PRODUCTNAME%>-Appliance importiert werden (siehe **Administration** 190 **Import** **Import S/MIME keys**).<br><br>Am E-Mail Client müssen in der Regel zwei LDAP Adressbücher erzeugt werden:<br>1. zur Abfrage der unternehmensinternen CA, welche das Schlüsselmaterial für die interne E-Mail Verschlüsselung bereit stellt<br>2. zur Abfrage des über diese Option aktivierten Key Servers der SEPPmail-Appliance<br>Hierzu ist es ausreichend die IP-Adresse beziehungsweise den Hostnamen der SEPPmail-Appliance sowie einen der Ports 387 oder 388, beziehungsweise 635 für eine verschlüsselte Verbindung anzugeben. Eine Authentifizierung ist nicht notwendig<br>Weiterhin wichtig ist, dass dem X.509 Root Zertifikat der internen CA der SEPPmail-Appliance (siehe **CA** 185 **Download certificate**) an den Clients vertraut wird.<br><br>(diese Option schliesst die folgende Option aus) |
| Enable ldap server on ports 388, 387 and 635 to distribute collected S/MIME certificates to internal users | Durch aktivieren dieser Option wird die OEM-PRODUCTNAME%>-Appliance und stellt somit die öffentlichen S/MIME Schlüssel per LDAP zur Verfügung.<br><br>(diese Option schliesst die vorhergehende Option aus) |
| Use Incamail instead of local GINA interface | Diese Option ist nur für Teilnehmer des schweizer Dienstes Incamail relevant. |

Die vorgenommenen Änderungen werden über die Schaltfläche **Save and Create ruleset** gespeichert. Das Ruleset wird mit den vorgenommen Einstellungen generiert.

### Sektion SMTP Ruleset

Über die Schalfläche **Display Ruleset** wird das Ruleset der OEM-PRODUCTNAME%>-Appliance angezeigt. Wurde dieses über den **Ruleset Generator** erzeugt, so steht in den ersten beiden Zeilen Datum und Uhrzeit der Erzeugung, sowie die Version, mit welcher das Ruleset erzeugt wurde.

In sehr grossen Unternehmen mit entsprechend umfangreichen individuellen Anforderungen besteht

© 2015 SEPPmail AG

die Möglichkeit ein Ruleset mittels der **Referenz der Regelwerk-Anweisungen** 228 zu erstellen. Dieses kann über die Schaltfläche **Upload** importiert und verwendet werden.

© 2015 SEPPmail AG

### 7.6.1 Untermenü Create new GINA Domain

**Sektion** Create new GINA Domain

| Parameter | Beschreibung |
|---|---|
| Description | Hier ist der Name einzugeben, welcher im Auswahlmenü Mail Processing 147 GINA Domains angezeigt werden soll. |
| Hostname | Ist unter Mail Processing 147 GINA Settings die Option "Use virtual hosting" aktiviert, so ist hier der FQDN anzugeben, unter welchem das Interface erreichbar sein wird (zum Beispiel securemail.meinkunde.ch).<br>Andernfalls ist hier der Name des Unterverzeichnisses anzugeben, in welchem das GINA-Interface erzeugt werden soll (zum Beispiel meinkunde).<br>Das neue GINA-Interface wird dann im Unterverzeichnis des unter dem FQDN des [default]-GINA-Eintrages erreichbar sein (zum Beispiel https://securemail.meinefirma.ch/meinkunde/web.app) |

Über die Schaltfläche Create wird der Vorgang abgeschlossen.

© 2015 SEPPmail AG

### 7.6.2 Untermenü Edit GINA Settings

In diesem Menü können die Einstellungen für die gewählte GINA-Domain individuell vorgenommen werden.
Zusätzlich zu den technischen Einstellungen kann über die Schaltfläche **Edit GINA Layout** jeweils das Design an die Firmenidentität angepasst werden (siehe **Edit GINA Layout** 172).

**Sektion Secure GINA Host**

| Parameter | Beschreibung |
|---|---|
| **Hostname** | Ist unter **Mail Processing** 147 **GINA Settings** die Option "Use virtual hosting" aktiviert, so ist hier der FQDN anzugeben, unter welchem das Interface erreichbar sein wird (zum Beispiel securemail.meinkunde.ch).<br>Andernfalls ist hier der Name des Unterverzeichnisses anzugeben, in welchem das GINA-Interface erzeugt werden soll (zum Beispiel meinkunde).<br>Das neue GINA-Interface wird dann im Unterverzeichnis des unter dem FQDN des [default]-GINA-Eintrages erreichbar sein (zum Beispiel https://securemail.meinefirma.ch/meinkunde/web.app).<br> **Hinweis:**<br>**Der hier eingetragene FQDN muss aus dem Internet erreichbar sein. Das heisst entsprechender DNS Eintrag muss veranlasst werden.** |

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

**Sektion Master Template**

Diese Sektion erscheint nur, falls ein anderes als das [default] GINA-Interface editiert wird.

| Parameter | Beschreibung |
|---|---|
| **Master Template** | Durch Auswahl eines Master Templates können teilweise in den folgenden Sektionen wahlweise die Einstellungen des anderen GINA-Interface übernommen werden. |

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

**Sektion Admin**

Einstellungen für den Versand von GINA-Systemmeldungen.

| Parameter | Beschreibung |
|---|---|
| **Use settings from master template** | Diese Option erscheint nur, falls ein anderes als das [default] GINA-Interface editiert wird.<br>Durch Aktivieren dieser Option werden die Einstellungen aus der unter **Master Template** gewählten Vorlage verwendet.<br>Eventuell vorgenommene Änderungen der weiteren Konfigurationspunkte |

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| | dieser Sektion bleiben ohne Auswirkung. |
| Admin E-mail | An die hier eingegebene E-Mail-Adresse werden Passwort-Anfragen von GINA-Benutzern des entsprechenden GINA-Interfaces weitergeleitet. Ebenso wird diese E-Mail-Adresse als Absender der GINA-Passwort- und Aktivierungs E-Mails verwendet.<br><br>Bleibt dieses Feld leer, so wird die Passwort-Anfrage eines GINA-Benutzers an den Internen Absender weitergeleitet, der dem entsprechenden GINA-Benutzer über diese Technologie eine E-Mail gesendet hat.<br>Als Absender der Passwort-E-Mails wird ebenfalls der interne Absender der GINA-Mail verwendet. |
| **Send password reset e-mails to original sender instead of Admin E-mail address** | In speziellen Konstellationen können bei leerer Admin E-mail und den daraus resultierenden Versand von GINA-Paswwort-/Aktivierungs-E-Mails im Namen des internen Absenders Probleme auftreten. In diesen Fällen ist zwingend eine Admin E-mail einzutragen. Soll dennoch bei Passwort-Reset-Anfragen der ursprüngliche Absender anstatt des eingetragenen Admins benachrichtigt werden, so ist an sieser Stelle der Haken zu setzen. |

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

### Sektion Extended settings

Grundlegende Einstellungen für die über das GINA-Webinterface zur Verfügung gestellten Funktionen.

| Parameter | Beschreibung |
|---|---|
| **Use settings from master template** | Diese Option erscheint nur, falls ein anderes als das [default] GINA-Interface editiert wird.<br>Durch Aktivieren dieser Option werden die Einstellungen aus der unter **Master Template** gewählten Vorlage verwendet.<br>Eventuell vorgenommene Änderungen der weiteren Konfigurationspunkte dieser Sektion bleiben ohne Auswirkung. |
| **Default Forward Page** | Sollte die URL der GINA-Seite ohne den Zusatz "/web.app" aufgerufen werden, kann an dieser Stelle auf eine andere Seite - zum Beispiel die Homepage des Unternehmens - weitergeleitet werden.<br>Soll dennoch auf das GINA-Interface weitergeleitet werden, so ist die URL einzugeben, wie sie oberhalb der Eingabezeile angezeigt wird.<br>Bleibt man beim Beispiel aus der Sektion **Secure GINA Host** würde dort folgendes stehen:<br>**Note:** If you want to show the GINA login page by default, enter "https://securemail.meinefirma.ch/meinkunde/web.app" (without the quotes) |
| **Always zip HTML attachments when encrypting mail with GINA technology** | Bei aktiver Option wird der verschlüsselte HTML Anhang der GINA-Mail in eine ZIP Datei gepackt. Dies wird für die Kompatibilität zu älteren OWA Versionen benötigt. Für einzelne E-Mails kann die Steuerung dieser Funktion durch das Betreffzeilen Schlüsselwort [zip] vorgenommen werden. |

© 2015 SEPPmail AG

| | |
|---|---|
| **"Send copy to myself" checked by default when writing GINA mails** | Mit dieser Option wird der Haken im %OEM-WEBMAIL-GINA%>-Interface für eine Kopie an den Sender bereits als Standard gesetzt.<br>Dadurch erhält der GINA-Benutzer beim Versenden einer E-Mail diese ebenfalls als GINA-Mail in Kopie und hat somit einen entsprechenden Nachweis. |
| **Sender always receives notification when recipient readsGINA mails** | Mit dem Setzen dieses Hakens wird die Anforderung einer Lesesbestätigung beim Versand von GINA-Mails als Standard definiert.<br>Eventuell vom Absender definierte Einstellungen dadurch überschrieben. |
| **Allow account self-registration in GINA portal without initial mail** | Erlaubt Personen, welche sich auf dasGINA-Interface (im Beispiel aus der Sektion **Secure GINA Host** "https://securemail.meinefirma.ch/meinkunde/web.app") verbinden eine Registrierung ohne initialer GINA-Mail.<br>Somit wird einem externen Kommunikationspartner ermöglicht, eine sichere E-Mail-Kommunikation über das GINA-Interface initial zu starten. Voraussetzung hierfür ist, dass ihm auch eine gültige E-Mail-Adresse innerhalb der E-Mail-Domäne des SEPPmail-Betreibers bekannt ist.<br>Dies bedingt auch das Aktivieren der Option **Allow GINA users to write new mails**. |
| **Enable S/MIME certificate / openPGP key search and management in GINA** | Hierdurch wird dem angemeldeten GINA-Benutzer erlaubt, nach öffentlichen S/MIME beziehungsweise openPGP Schlüsseln von internen SEPPmail-Benutzern über dasGINA-Portal zu suchen. |
| **Allow download of public domain keys/ domain certificates** | Mit dieser Option wird zusätzlich die Suche von öffentlichen **Domänen** Schlüsseln der auf der SEPPmail-Appliance verwalteten E-Mail-Domänen zu suchen. |
| **Allow unregistered users to search public keys/ certificates of internal users** | Wird dieser Haken gesetzt, so wird die Schlüssel Suche nicht nur angemeldeten GINA-Benutzern, sondern jedem der sich auf das GINA>-Portal verbindet, erlaubt.<br>Da im GINA-Interface für eine Schlüssel Suche immer die E-Mail-Adresse des Empfängers eingegeben werden muss, ist ein Adress-Harvesting nicht möglich. |
| **Allow GINA users to write new mails** | Diese Option erlaubtGINA-Benutzern initial E-Mails an Empfänger innerhalb der E-Mail-Domäne des SEPPmail-Betreibers zu senden und nicht nur auf erhaltene GINA-Mails zu Antworten. |
| **Do not allowGINA users to edit recipient when replying to e-mails** | Mit diesem Parameter wird festgelegt, ob Empfänger von GINA-Mails beim Antworten den oder die Empfänger editieren dürfen. |
| **Allow GINA users to reply to external recipients of GINA messages** | Erlaubt es einen GINA-Benutzer an alle Empfängern einer GINA-E-Mail - auch externen, also denen, die nicht der E-Mail-Domäne des ursprünglichen Absenders angehören - zu antworten. |

© 2015 SEPPmail AG

| | |
|---|---|
| | **Hinweis:**<br>**Wurde diese Option gewählt, so können bei gleichzeitig deaktivierter Option "Do not allowGINA users to edit recipient when replying to e-mails" nur bereits vorhanden Empfänger durch den GINA-Benutzer entfernt, jedoch keine weiteren hinzugefügt werden.** |
| SMTP sender address for sending to external recipients: | Da der Versand der E-Mails an externe Empfänger mit einer existenten E-Mail-Adresse der lokalen E-Mail-Domäne erfolgen muss (Stichwort SPF Prüfung), ist die Versender-Adresse für die oben genannten Antwort-E-Mails hier einzutragen.<br>**Hinweis:**<br>**Die hier angegebene E-Mail-Adresse erhält gegebenenfalls Systembenachrichtigungen wie Bounce- oder Non Delivery Report (NDR) E-Mails.** |
| **Allow messages to be downloaded as Outlook message (.msg) files** | Mit Aktivieren dieser Option wird dem Empfänger einer GINA-Mail im GINA-Interface eine Schaltfläche zum Download der E-Mail im msg-Format - also Outlook - angeboten. Somit wird der Empfänger in die Lage versetzt die ursprünglich GINA-verschlüsselte E-Mail in Outlook im Klartext abzuspeichern.<br>**Hinweis:**<br>**Wird nach abspeichern der Nachricht im Klartext über die "Antworten" Schaltfläche im Outlook geantwortet, so geschieht dies unverschlüsselt!** |
| **Allow messages to be downloaded as MIME (.eml) files** | Mit Aktivieren dieser Option wird dem Empfänger einer GINA-Mail im GINA-Interface eine Schaltfläche zum Download der E-Mail im eml-Format für den Import in einen E-Mail-Client angeboten. Somit wird der Empfänger in die Lage versetzt die ursprünglichGINA-verschlüsselte E-Mail in seinem E-Mail-Client im Klartext abzuspeichern.<br>**Hinweis:**<br>**Wird nach abspeichern der Nachricht im Klartext über die "Antworten" Funktion des E-Mail-Clients geantwortet, so geschieht dies unverschlüsselt!** |
| **When encrypting mail with GINA technology, use text-only emails** | Versendet GINA-Mail im Text- statt im HTML-Format.<br>Dies kann gegebenenfalls notwendig sein, wenn ein Empfänger den Empfang von HTML-Mails nicht zulässt. |

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

**Sektion Large File Management**

Einstellungen für die Übertragung grosser Dateien. Diese Option steht nur zur Verfügung, wenn Large File Management (LFM) lizensiert und aktiviert wurde.

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| **Use settings from master template** | Diese Option erscheint nur, falls ein anderes als das [default] GINA-Interface editiert wird.<br>Durch Aktivieren dieser Option werden die Einstellungen aus der unter **Master Template** gewählten Vorlage verwendet.<br>Eventuell vorgenommene Änderungen der weiteren Konfigurationspunkte dieser Sektion bleiben ohne Auswirkung. |
| **Enable Large File Messages without authentication** | Mit dem Betreffzeilen-Schlüsselwort [lfm:nocrypt] kann der Absender bei aktivierter Option steuern, dass der Empfänger zur Abholung des LFM-Anhangs kein Passwort am GINA-Webinterface eingeben muss. |
| **Enable Large File Management** | Mit dem Anhaken dieser Option wird das Large File Management (LFM) aktiviert. LFM ist eine Zusatzoption und muss somit auch separat lizensiert werden. |
| **How long (in days) to store Large Files** | Hier wird die Verweildauer - in Tagen - von LFM-Mails angegeben. Der Empfänger bekommt das Verfallsdatum im Betreff der GINA-Benachrichtigungs-Mail mitgeteilt. Die Einstellung "0" null bedeutet, dass LFM Mails nie gelöscht werden.<br>Es ist darauf zu achten, dass genügend Speicher auf dem System zur Verfügung steht, anndernfalls würden LFM Mails abgewiesen (bounced). |
| **Size (in KB) above which messages are treated as Large Files** | Gibt die Grenze - in kB - an, ab wann eine E-Mail als LFM Mail behandelt wird. Dabei gilt zu beachten, dass Anhänge in E-Mails aufgrund der BASE-64 Codierung bis um die Hälfte grösser sein können, als im Dateisystem. |
| **Maximum size (in KB) for LFM messages** | Gibt eine Maximalgrösse für LFM Dateien an. Wird hier "0" (null) einegegeben, so wird kein Limit vorgegeben. |
| **Limit Large Files per day and user** | Limitiert die Anzahl von LFM Mails, die ein einzelner Benutzer pro Tag versenden darf. Die Einstellung "0" null bedeutet kein Limit. |

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

### Sektion Terms of use

Einstellungen bezüglich Allgemeiner Geschäftsbedingungen.

| Parameter | Beschreibung |
|---|---|
| **Use settings from master template** | Diese Option erscheint nur, falls ein anderes als das [default] GINA-Interface editiert wird.<br>Durch Aktivieren dieser Option werden die Einstellungen aus der unter **Master Template** gewählten Vorlage verwendet.<br>Eventuell vorgenommene Änderungen der weiteren Konfigurationspunkte dieser Sektion bleiben ohne Auswirkung. |
| **Require new users to accept terms of use** | Nach Empfang der initialen GINA-Mail wird der Empfänger beim Registrierungsprozess aufgefordert, die Allgemeinen Geschäftsbedingungen zu akzeptieren. |

© 2015 SEPPmail AG

| | | |
|---|---|---|
| | **Terms of use URL** | Eingabe der URL zu den Allgemeinen Geschäftsbedingungen, zum Beispiel https://www.ihrefirma.ch/agb. |

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

### Sektion Language Settings

Spracheinstellungen des GINA-Webinterfaces und dessen Benachrichtigungen.

<table>
<tr><th colspan="3">Parameter</th><th colspan="2">Beschreibung</th></tr>
<tr><td colspan="3">Use settings from master template</td><td colspan="2">Diese Option erscheint nur, falls ein anderes als das [default] GINA-Interface editiert wird.<br>Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master Template gewählten Vorlage verwendet.<br>Eventuell vorgenommene Änderungen der weiteren Konfigurationspunkte dieser Sektion bleiben ohne Auswirkung.</td></tr>
<tr><td colspan="3">Default language:</td><td colspan="2">Über das Auswahlmenü wird die Standard-Sprache für das jeweilige GINA-Interface gewählt. Diese Sprache fuss im folgenden Menüpunkt auch als Verfügbar (Enabled) markiert sein.</td></tr>
<tr><td colspan="3">Available Languages:</td><td colspan="2">Bei der Auswahl der Sprachen gilt zu beachten, dass mit jeder weiteren Sprache die Länge der GINA-Mail sowie bei initialen E-Mails die Länge der Passwort-Mails zunimmt.</td></tr>
<tr><td></td><td>Language</td><td>Enabled</td><td rowspan="8">Über die Schalfläche Edit translations öffnet das Menü Edit Translations 176 der jeweiligen Sprache, über welches die Texte aller GINA-Komponenten individuell angepasst werden können.</td><td rowspan="8">Über die Schaltfläche Download kann die jeweilige Sprachdatei heruntergeladen werden. Wird diese im Anschluss angepasst, so kann Sie über die [default] GINA-Einstellungen wieder hochgeladen werden.</td></tr>
<tr><td></td><td>German (d)</td><td rowspan="7">Aktiviert oder deaktiviert die jeweilige Sprache</td></tr>
<tr><td></td><td>Enfglish (e)</td></tr>
<tr><td></td><td>French (f)</td></tr>
<tr><td></td><td>Italian (i)</td></tr>
<tr><td></td><td>Spanish (s)</td></tr>
<tr><td></td><td>Dutch (n)</td></tr>
<tr><td></td><td>Polish (p)</td></tr>
</table>

Wird das [default] GINA-Interface editiert, so können über die Schaltfläche **Add new** weitere Sprachen hinzugefügt werden. Für das Erstellen einer neuen Sprachdatei ist der einfachste Weg, eine bereits vorhandene über die Schaltfläche **Download** (siehe Tabelle oben) herunterzuladen, zu übersetzen und über die Schaltfläche **Add new** wieder hochzuladen.

Die vorgenommenen Änderungen werden über die Schaltfläche **Save** gespeichert.

### Sektion Security

In dieser Sektion werden die Passwort-Kriterien sowie die Möglichkeiten zur Passwort-Rücksetzung

© 2015 SEPPmail AG

angegeben.

| Parameter | Beschreibung |
|---|---|
| **Use settings from master template** | Diese Option erscheint nur, falls ein anderes als das [default] GINA-Interface editiert wird.<br>Durch Aktivieren dieser Option werden die Einstellungen aus der unter **Master Template** gewählten Vorlage verwendet.<br>Eventuell vorgenommene Änderungen der weiteren Konfigurationspunkte dieser Sektion bleiben ohne Auswirkung. |
| **Choose how the user can retrieve lost passwords** | Auswahl der Passwort-Rücksetzungs-Möglichkeiten des GINA-Benutzers.<br>Die Passwort-Rücksetzung per SMS ist nur bei lizensiertem Self-Service-Password-Management (SSPM) verfügbar. |
| **default** | Standard Einstellung. Diese entspricht der Opton "Reset by Hotline". |
| **Reset by Email verification** | Der GINA-Benutzer direkt nach dem Beantworten seiner Sicherheitsfrage aufgefordert ein neues Passwort einzugeben. |
| **Reset by hotline** | Der GINA-Benutzer erhält nach dem Beantworten seiner Sicherheitsfrage die Aufforderung zur Eingabe einer Telefonnummer für den Rückruf durch die Hotline. |
| **Reset by hotline, no reminder question/ answer** | Der GINA-Benutzer wird ohne Sicherheitsfrage zur Eingabe einer Telefonnummer für den Rückruf durch die Hotline aufgefordert.<br>Dies funktioniert jedoch nur, wenn das GINA-Interface über über eine GINA-Mail aufgerufen wurde, also nicht durch die blosse Anmeldung. |
| **Reset by SMS** | Dem GINA-Benutzer wird nach dem Beantworten seiner Sicherheitsfrage seine hinterlegte Handynummer angezeigt. An diese wird nach Bestätigung durch den Benutzer eine Passwort-SMS gesendet.<br>Ist für den Benutzer keine Handynummer hinterlegt, wird zur Eingabe einer Telefonnummer für den Rückruf durch die Hotline aufgefordert.<br>**Für diese Option muss das Self-Service-Password-Management (SSPM) lizensiert sein!** |
| **Let user choose between hotline and SMS** | Nach dem Beantworten seiner Sicherheitsfrage kann der GINA-Benutzer wählen, ob das neue Passwort per SMS an seine Handynummer gesendet werden soll, sofern diese bereits hinterlegt ist, oder ob er eine Telefonnummer für den Rückruf durch die Hotline eingeben will.<br>**Für diese Option muss das Self-Service-Password-Management (SSPM) lizensiert sein!** |
| **Minimum password length:** | Gibt die minimale Passwort Länge an. Mögliche Werte liegen zwischen 4 und 16 |
| **Must contain at least one lower case letter** | Passwort muss mindestens einen Kleinbuchstaben enthalten. |
| **Must contain at least one upper case letter** | Passwort muss mindestens einen Grossbuchstaben enthalten. |
| **Must contain at least one number** | Passwort muss mindestens eine Ziffer enthalten. |

© 2015 SEPPmail AG

| | | |
|---|---|---|
| | **Must contain at least one special character** | Passwort muss mindestens eine Sonderzeichen enthalten. |
| | **Must not contain own name or mail address** | Passwort darf nicht die eigene E-Mail-Adresse enthalten. |
| | **Must be different from previous  password (s)** | Passwort muss sich von den letzten n Passwörtern unterscheiden. |
| | **Must be changed at least every  days** | Passwort muss nach n Tagen geändert werden. |

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

**Sektion Certificate Login**

Ermöglicht die Anmeldung an GINA-Portal mittels Zertifikat. Hierfür muss das Rootzertifikat der CA, welche die Login Zertifikate ausstellt in das Eingabefeld eingefügt werden.

| Parameter | Beschreibung |
|---|---|
| **Use settings from master template** | Diese Option erscheint nur, falls ein anderes als das [default] GINA-Interface editiert wird.<br>Durch Aktivieren dieser Option werden die Einstellungen aus der unter Master Template gewählten Vorlage verwendet.<br>Eventuell vorgenommene Änderungen der weiteren Konfigurationspunkte dieser Sektion bleiben ohne Auswirkung. |

Der zugreifende Benutzer muss sein entsprechendes Benutzer-Zertifikat in seinem Browser installiert haben.
Sollte mehr als ein GINA-Interface konfiguriert werden, so ist für diese Art des LogIns die Option "Use virtual hosting" (siehe Mail Processing 147 GINA Settings) zu verwenden.
Weiterhin ist diese Option nicht mit der Einstellung "System GINA https Protocol **Enable local https proxy**" kompatibel.

Die vorgenommenen Änderungen werden über die Schaltfläche Save gespeichert.

### 7.6.2.1 Untermenü Edit GINA Layout

**Sektion Company Logo**

| Parameter | Beschreibung |
|---|---|
| **Use settings from master template** | Diese Option erscheint nur, falls ein anderes als das [default] GINA-Interface editiert wird.<br>Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe Edit GINA Settings 165 Sektion Master Template) verwendet.<br>Eventuell vorgenommene Änderungen der weiteren Konfigurationspunkte dieser Sektion bleiben ohne Auswirkung. |

© 2015 SEPPmail AG

| | |
|---|---|
| | Ist bereits ein Logo importiert, so wird dieses hier angezeigt.<br>Über die Browser-Schaltfläche Datei auswählen kann ein Logo im gif-Format zum Upload ausgewählt werden.<br>Die maximale Grösse des Logos ist vom verwendeten Cascaded Style Sheet (CSS) abhängig. Im Standard beträgt diese 200x55 Pixel. |

Über die Schaltfläche **Delete** wird das Logo-Bild gelöscht. Über die Schaltfläche **Save** wird das ausgewählte Bild gespeichert. Ist bereits ein Bild vorhanden, so wird dieses überschrieben.

**Sektion Header Logo (optional)**

| Parameter | Beschreibung |
|---|---|
| **Use settings from master template** | Diese Option erscheint nur, falls ein anderes als das [default] GINA-Interface editiert wird.<br>Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe Edit GINA Settings 165 Sektion Master Template) verwendet.<br>Eventuell vorgenommene Änderungen der weiteren Konfigurationspunkte dieser Sektion bleiben ohne Auswirkung. |
| | Ist bereits ein Kopfzeilen-Logo importiert, so wird dieses hier angezeigt.<br>Über die Browser-Schaltfläche Datei auswählen kann ein Logo im gif-Format zum Upload ausgewählt werden.<br>Die maximale Grösse des Logos ist vom verwendeten Cascaded Style Sheet (CSS) abhängig. Im Standard beträgt diese 120x80 Pixel.<br>**Das Header Logo wird nur angezeigt, wenn die Anzeige in den Extended Settings aktiviert wurde.** |

Über die Schaltfläche **Delete** wird das Logo-Bild gelöscht. Über die Schaltfläche **Save** wird das ausgewählte Bild gespeichert. Ist bereits ein Bild vorhanden, so wird dieses überschrieben.

**Sektion Favourites Icon (optional)**

| Parameter | Beschreibung |
|---|---|
| **Use settings from master template** | Diese Option erscheint nur, falls ein anderes als das [default] GINA-Interface editiert wird.<br>Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe Edit GINA Settings 165 Sektion Master Template) verwendet.<br>Eventuell vorgenommene Änderungen der weiteren Konfigurationspunkte dieser Sektion bleiben ohne Auswirkung. |
| | Ist bereits ein Favoriten-Icon importiert, so wird dieses hier angezeigt.<br>Über die Browser-Schaltfläche Datei auswählen kann ein Icon in den Formaten gif, png, jpeg und ico zum Upload ausgewählt werden.<br>Die maximale Grösse des Icons beträgt 16x16 Pixel. |

Über die Schaltfläche **Delete** wird das Logo-Bild gelöscht. Über die Schaltfläche **Save** wird das ausgewählte Bild gespeichert. Ist bereits ein Bild vorhanden, so wird dieses überschrieben.

© 2015 SEPPmail AG

**Sektion Footer Logo (optional)**

| Parameter | Beschreibung |
|---|---|
| **Use settings from master template** | Diese Option erscheint nur, falls ein anderes als das [default] GINA-Interface editiert wird.<br>Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe Edit GINA Settings 165 Sektion Master Template) verwendet.<br>Eventuell vorgenommene Änderungen der weiteren Konfigurationspunkte dieser Sektion bleiben ohne Auswirkung. |
| | Ist bereits ein Fusszeilen-Logo importiert, so wird dieses hier angezeigt.<br>Über die Browser-Schaltfläche Datei auswählen kann ein Logo im gif-Format zum Upload ausgewählt werden.<br>Die maximale Grösse des Logos ist vom verwendeten Cascaded Style Sheet (CSS) abhängig. Im Standard beträgt diese 120x80 Pixel.<br>**Das Fusszeilen-Logo wird nur angezeigt, wenn die Anzeige in den Extended Settings aktiviert wurde.** |

Über die Schaltfläche Delete wird das Logo-Bild gelöscht. Über die Schaltfläche Save wird das ausgewählte Bild gespeichert. Ist bereits ein Bild vorhanden, so wird dieses überschrieben.

**Sektion Bachkground Image (optional)**

| Parameter | Beschreibung |
|---|---|
| **Use settings from master template** | Diese Option erscheint nur, falls ein anderes als das [default] GINA-Interface editiert wird.<br>Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe Edit GINA Settings 165 Sektion Master Template) verwendet.<br>Eventuell vorgenommene Änderungen der weiteren Konfigurationspunkte dieser Sektion bleiben ohne Auswirkung. |
| | Ist bereits ein Hintergrundbild importiert, so wird dieses hier angezeigt.<br>Über die Browser-Schaltfläche Datei auswählen kann ein Bild im gif-Format zum Upload ausgewählt werden.<br>Im Standard Cascaded Style Sheet (CSS) wird kein Hintergrundbild verwendet. Soll dieses Eingebettet werden, so ist das CSS in der Sektion GINA CSS entsprechend anzupassen. |

Über die Schaltfläche Delete wird das Logo-Bild gelöscht. Über die Schaltfläche Save wird das ausgewählte Bild gespeichert. Ist bereits ein Bild vorhanden, so wird dieses überschrieben.

**Sektion GINA CSS**

| Parameter | Beschreibung |
|---|---|

© 2015 SEPPmail AG

| | |
|---|---|
| **Use settings from master template** | Diese Option erscheint nur, falls ein anderes als das [default] GINA-Interface editiert wird.<br>Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe Edit GINA Settings 165 Sektion Master Template) verwendet.<br>Eventuell vorgenommene Änderungen der weiteren Konfigurationspunkte dieser Sektion bleiben ohne Auswirkung. |
| GINA CSS: | Im Eingabefeld kann das Aussehen der GINA-Seiten per Cascaded Style Sheet (CSS) an das jeweilige Firmen Design angepasst werden.<br>Dabei ist zu beachten, dass für den GINA-Webmailer die individuell angepassten CSS erst nach den Standard Einstellungen geladen werden. Das heisst bei gleichlautenden Definitionen überschreibt das individuell angepasste CSS das Standard CSS.<br>Bei einer GINA-Mail wird bei Verwendung eines individuell angepassten CSS nur dieses geladen. Somit werden hier keine Elemnte aus dem Standard CSS verwendet. |

Über die Schaltfläche **Preview GINA** wird ein Beispiel der GINA-Anmeldeseite unter Verwendung der vorgenommen Konfiguration angezeigt .
Die Schaltfläche **Preview Secure email** generiert ein Beispiel für das Aussehen einer GINA-Mail unter Verwendung der vorgenommen Konfiguration.
Sollen die Standard SEPPmail Cascaded Style Sheet (CSS) wieder hergestellt werden, so ist die Schaltfläche **Restore default CSS** zu klicken.
Mittels **Save** werden die Änderungen am CSS gespeichert.

**Sektion Extended settings**

| Parameter | Beschreibung |
|---|---|
| **Use settings from master template** | Diese Option erscheint nur, falls ein anderes als das [default] GINA-Interface editiert wird.<br>Durch Aktivieren dieser Option werden die Einstellungen aus der gewählten Vorlage (siehe Edit GINA Settings 165 Sektion Master Template) verwendet.<br>Eventuell vorgenommene Änderungen der weiteren Konfigurationspunkte dieser Sektion bleiben ohne Auswirkung. |
| **Disable "Powered by ..." Logo in GINA viewer** | Deaktiviert das Hersteller Logo rechts unten auf der GINA-Seite. |
| **Enable Header logo on Login page** | Aktiviert das Kopfzeilen-Logo auf der GINA-Anmeldeseite. Dies setzt voraus, dass in der Sektion Header Logo auch ein Logo hochgeladen wurde. |
| **Enable Header logo on all other pages** | Aktiviert das Kopfzeilen-Logo auf allen weiteren GINA-Seiten. Dies setzt voraus, dass in der Sektion Header Logo auch ein Logo hochgeladen wurde. |
| **Enable Footer logo on Login page** | Aktiviert das Fusszeilen-Logo auf der GINA-Anmeldeseite. Dies setzt voraus, dass in der Sektion Footer Logo auch ein Logo hochgeladen wurde. |

© 2015 SEPPmail AG

| | |
|---|---|
| **Enable Footer logo on all other pages** | Aktiviert das Fusszeilen-Logo auf allen weiteren GINA-Seiten. Dies setzt voraus, dass in der Sektion **Footer Logo** auch ein Logo hochgeladen wurde. |
| **Enable Footer text on Login page** | Aktiviert die Fussnote auf der GINA-Anmeldeseite. Dies setzt voraus, dass in der Sektion **Footer text** aus dem Sub-Menü **Edit Translations** 176 auch ein Fussnoten Text hinterlegt wurde. |
| **Enable Footer text on all other pages** | Aktiviert die Fussnote auf allen weiteren GINA-Seiten. Dies setzt voraus, dass in der Sektion **Footer text** aus dem Sub-Menü **Edit Translations** 176 auch ein Fussnoten Text hinterlegt wurde. |

Über die Schaltfläche **Save** werden die Einstellungen gespeichert.

#### 7.6.2.2 Untermenü Edit Translations

In den folgenden Sektionen sind in den Eingabefeldern jeweils bereits die Standardtexte der gewählten Sprache enthalten.
Diese Texte können nach Bedarf angepasst oder ersetzt werden.

**Sektion Customization**

Diese Sektion beinhaltet Syntax-Hinweise für das Bearbeiten der Sprachdatei.
Weiterhin sind folgende Variablen zulässig:

- @email@ E-Mail Adresse des Empfängers der GINA-Mail
- @sender@ Absender der GINA-Mail
- @subject@ ursprünglicher Betreff der zu versendenden E-Mail

**Sektion Text in GINA**

In dieser Sektion wird der Textkörper für der GINA-Mail an den Empfänger definiert.

| **Beschreibung** |
|---|
| Das erste Eingabefeld definiert eine Überschrift für den im zweiten Eingabefeld folgenden Text. Diese wird im Standard fett dargestellt. |
| Im zweiten Eingabefeld folgt die Beschreibung, wie der Empfänger vorzugehen hat um die anhängende Originalnachricht entschlüsseln zu können. |

Mittels **Save** werden Änderungen gespeichert. Über **Restore default** wird der Standard-Inhalt der Sektion in der Sprachdatei wieder hergestellt.

**Sektion Open hint in GINA**

Das hier zur Verfügung stehende Textfeld definiert die Beschreibung, welche nach dem öffnen des HTML-Anhangs (secure-email.html) unterhalb der Schaltfläche "OK" angezeigt wird.
Die Beschreibung sollte aufzeigen, welche Aktion(en) durch das Klicken von "OK" ausgelöst werden.

Mittels **Save** werden Änderungen gespeichert. Über **Restore default** wird der Standard-Inhalt der der Sektion in der Sprachdatei wieder hergestellt.

© 2015 SEPPmail AG

**Sektion Greeting on Login page**

| Beschreibung |
| --- |
| Das erste Eingabefeld definiert eine Überschrift für den im zweiten Eingabefeld folgenden Text. Diese wird im Standard fett dargestellt. |
| Im zweiten Eingabefeld folgt die Beschreibung, wie der Empfänger vorzugehen hat um die anhängende Originalnachricht entschlüsseln zu können. |

Mittels **Save** werden Änderungen gespeichert. Über **Restore default** wird der Standard-Inhalt der der Sektion in der Sprachdatei wieder hergestellt.

**Sektion Footer text**

Die Eingabe eines Fussnotentextes ist optional. Das Aktivieren der Anzeige des Fussnotentextes muss unter **Edit GINA Layout** 172 in der Sektion **Extended settings** erfolgen.

Mittels **Save** werden Änderungen gespeichert. Über **Restore default** wird der Standard-Inhalt der der Sektion in der Sprachdatei wieder hergestellt.

**Sektion GINAPassword Notification Mail**

| Beschreibung |
| --- |
| Die erste Zeile beinhaltet den Text, welcher in der Betreffzeile der Passwort Benachrichtigungsmail enthalten sein soll.<br>Am Ende dieses Textes wird beim Versand der Password Benachrichtigungsmal ein Leerzeichen und die E-Mail-Adresse des Empfängers der GINA-Mail automatisch eingefügt. |
| Die zweite Zeile beinhaltet den E-Mail Text der Passwort Benachrichtigungsmail.<br>Dieser Text beginnt mit der Wiederholung der Betreffzeile. Im Anschluss wird der Text aus Textfeld eingefügt und am Schluss eine Zeile mit dem Passort in der Form "Passwort: <Initialpasswort>" angefügt. |

Mittels **Save** werden Änderungen gespeichert. Über **Restore default** wird der Standard-Inhalt der der Sektion in der Sprachdatei wieder hergestellt.

**Sektion Edit Translation file**

Über die Schaltfläche **Advanced View** öffnet die Sektion **Edit Translation file**, welche den Umgang mit dem Editor beschriebt und weitere Syntax-Hinweise aufgeführt.
Das Eingabefeld des Editors beinhaltet bereits den Text der Standard-Sprachdatei für die gewählte Sprache zur Anpassung an die individuellen Bedürfnisse.

Mittels **Save** werden Änderungen gespeichert. Über **Restore default** wird der Standard-Inhalt der kompletten Sprachdatei wieder hergestellt.

Über die Schaltfläche **Normal View** wird zur vorherigen Ansicht zurück gewechselt.

© 2015 SEPPmail AG

### 7.6.3 Untermenü Edit Disclaimer

Wird der Standardtext angepasst oder ausgetauscht, so hat dies in beiden Sektionen zu erfolgen.

**Sektion Disclaimer as text**

Im Eingabefeld ist der Standardtext in deutsch und englisch bereits vorhanden. Dieser kann den individuellen Bedürfnissen angepasst oder vollständig ersetzt werden.

**Sektion Disclaimer as Html**

Im Eingabefeld ist der Standardtext im HTML-Code in deutsch und englisch bereits vorhanden. Bei Bedarf kann Aussehen und Text durch unterschiedliche HTML-Tags zur Formatierung (zum Beispiel Absätze, Schriftgrösse oder Schriftfarbe) individuell angepasst werden.

© 2015 SEPPmail AG

## 7.7 SSL

Im Menüpunkt **SSL** wird das Zertifikat angezeigt, welches für den SSL-Zugang auf das GINA- beziehungsweise auf die Administrations-Oberfläche verwendet wird. Dieses Zertifikat wird auch für die TLS-Verschlüsselung zu anderen Systemen verwendet.

Eine Ausnahme besteht bei Verwendung der Option "Use virtual hosting" aus der Sektion **GINA Settings** des Menüs **Mail Processing** 147, da hier für jede GINA-Domain ein eigenes Zertifikat einzubinden ist.

Ist bereits ein Zertifikat eingebunden, so wird dieses wie folgt angezeigt.
Andernfalls kann über die Schaltfläche **Request a new Certificate...** ein Zertifikat importiert, oder gegebenfalls ein Self-Signed-Zertifikat erzeugt werden. Das Verwenden eines Self-Signed-Zertifikat empfiehlt sich jedoch nur auf Test Systemen, da hierdurch die Zertifikatsprüfung des Internetbrowsers eines GINA-Mail-Empfangers beim Verbinden auf die Appliance fehlschlagen würde.

Über die Schaltfläche **Backup Certificate** kann das vorhandene SSL-Zertifikat im pem-Format exportiert werden (privater und öffentlicher Schlüssel sowie gegebenenfalls Zwischenzertifikate)

### Sektion Issued To

Diese Sektion zeigt Informationen über den Inhaber des SSL-Zertifikates.
Abhängig vom Zertifikat müssen nicht alle hier aufgeführten Parameter vorhanden sein.

| Parameter | Beschreibung |
|---|---|
| **Name (CN)** | In der Regel beinhaltet dieses Feld den Domänennamen, über welchen das GINA-Interface zu erreichen ist, zum Beispiel "securemail.firma.ch". Wird ein sogenanntes Wildcard-Zertifikat verwendet, so würde der Domänenname "*. firma.ch" lauten.<br>Bei Self-Signed-Zertifikaten kann hier zum Beispiel auch "firma.local" oder auch eine IP-Adresse, zum Beispiel "10.0.0.10" stehen. |
| **E-Mail Address** | In der Regel der wird die E-Mail-Adresse des Antragstellers, beziehungsweise des Verwalters des Zertifikates oder dessen Abteilung eingetragen. |
| **Org. Unit (OU)** | Organisationseinheit wie zum Beispiel ein Abteilungsname wie "Buchhaltung" |
| **Organization (O)** | Gibt die Organisation an, für welche das Zertifikat ausgestellt wurde, zum Beispiel "Firma" |
| **Locality (L)** | Standort zum Beispiel eine Stadt wie "Neuenhof" oder auch ein Teilgebäude wie "Werk2" |
| **State (ST)** | Bundesland, Kanton, Provinz oder Ähnliches, zum Beispiel "AG" für "Aargau" |
| **Country (C)** | Land, zum Beispiel "CH" für "Schweiz" |
| **Serial No.** | Seriennummer des Zertifikats |

### Sektion Issued By

Diese Sektion zeigt Informationen über den Aussteller des SSL-Zertifikates (Root-Zertifikat).
Abhängig vom Aussteller müssen nicht alle hier aufgeführten Parameter vorhanden sein.

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| **Name (CN)** | Name der ausstellenden Zertifizierungsstelle |
| **E-Mail Address** | In der Regel eine E-Mail-Adresse für Supportanfragen an den Aussteller |
| **Org. Unit (OU)** | Gibt eine Organisationseinheit des Ausstellers an |
| **Organization (O)** | Gibt die ausstellende Organisation an |
| **Locality (L)** | Gibt den Standort des Ausstellers an |
| **State (ST)** | Gibt ein Bundesland, Kanton, Provinz oder Ähnliches des Ausstellers an |
| **Country (C)** | Gibt das Land des Ausstellers an |
| **Serial No.** | Seriennummer des Zertifikats |

**Sektion Validity**
Zeigt die Gültigkeit des Zertifikates.

| Parameter | Beschreibung |
|---|---|
| **Issued on** | Ausstelldatum des SSL-Zertifikates |
| **Expires on** | Ablaufdatum des SSL-Zertifikates |

**Sektion Fingerprint**

Gibt den Hash des Zertifikates an.

| Parameter | Beschreibung |
|---|---|
| **Hashalgorhytmus des Zertifikates, zum Beispiel SHA1** | Der Fingerprint dient zur Überprüfung eines Zertifikats. Beispiel eines ein SHA1 Fingerprints: 48:2D:99:B1:64:C1:14:9C:B3:F2:C0:8D:FA:7F:40:9F:22:F5:11:F5 |

© 2015 SEPPmail AG

### 7.7.1 Untermenü Request a new Certificate

An dieser Stelle kann ein Self-Signed-Zertifikat ( in der Regel nur für Testzwecke) oder ein sogenannter Certificate Signing Request (CSR) erstellt werden.
Wird ein CSR erstellt, so wird das Schlüsselpaar auf der Appliance generiert, und nur der öffentliche Schlüssel in eine csr-Datei geschrieben, welche bei einer CA zur Signierung eingereicht und als Zertifikat zurückgegeben wird.
Ist bereits ein passendes SSL-Zertifikat vorhanden, so kann dieses in der Sektion **Upload existing key** importiert werden.

**Hinweis:**
Falls im oberen Bereich des Menüs die gelb hinterlegte Information **Remember to import the signed certificate** angezeigt wird, so wurde zuvor bereits ein Zertifikatsantrag erstellt.

Das neu erstellte SSL-Device-Zertificate sollte zusammen mit den gegebenenfalls zusätzlich benötigten Zwischen- oder auch Intermediate- CA-Zertifikate(n) und dem Zertifikat der Root-CA selbst in der Reinhenfolge

1. Public Key des eigenen SSL-Device-Zertifikats
2. Public Key von einer oder mehreren Intermediate CA-Zertifikaten
3. Public Key der Root-CA

eingefügt werden
Im Fehlerfall ist das SSL-Device-Zertifikat nicht zu nutzen. Ebenfalls kann dies zu Problemen beim Zugriff auf die Konfigurationsoberfläche führen. Für diesen Fall sollte sicherheitshalber vor dieser Aktion temporär der HTTP-Port (siehe **System Advanced View GUIProtocol** HTTP Port) für den Zugriff auf die Administrationsoberfläche (http://<Appliance>:8080) freigegeben werden.

**Sektion Issued To**

In dieser Sektion gibt der SSL-Zertifikats-Anforderer seine entsprechenden Informationen an.

| Parameter | Beschreibung |
|---|---|
| Name (CN) | In der Regel beinhaltet dieses Feld den Domänennamen, über welchen das GINA-Interface zu erreichen ist, zum Beispiel "securemail.firma.ch". Wird ein sogenanntes Wildcard-Zertifikat angefordert werden, so würde der Domänenname "*.firma.ch" lauten.<br>Bei Self-Signed-Zertifikaten kann hier zum Beispiel auch "firma.local" oder auch eine IP-Adresse, zum Beispiel "10.0.0.10" stehen. |
| E-Mail Address | In der Regel der wird die E-Mail-Adresse des Antragstellers, beziehungsweise des Verwalters des Zertifikates oder dessen Abteilung eingetragen. |
| *Org. Unit (OU)* | Organisationseinheit wie zum Beispiel ein Abteilungsname wie "Buchhaltung" |
| *Organization (O)* | Gibt die Organisation an, für welche das Zertifikat ausgestellt wurde, zum Beispiel "Firma" |
| *Locality (L)* | Standort zum Beispiel eine Stadt wie "Neuenhof" oder auch ein Teilgebäude wie "Werk2" |
| *State (ST)* | Bundesland, Kanton, Provinz oder Ähnliches, zum Beispiel "AG" für "Aargau" |
| **Country (C)** | Auswahl des Landes über das Drop-Down-Menü |

© 2015 SEPPmail AG

### Sektion Attributes

| Parameter | Beschreibung |
|---|---|
| **Key size (bits)** | Über das Drop-Down-Menü lässt sich die gewünschte Schlüssellänge für das Angeforderte Zertifikat einstellen. In der Regel ist hier die längste Schlüssellänge zu wählen, um dem jeweils aktuellen Sicherheitsstandard zu entsprechen. |
| **Signature** | Über das Drop-Down-Menü lässt sich auswählen, ob ein Self-Signed-Zertifikat oder ein CSR generiert werden soll.<br>Wird ein Self-Signed-Zertifikat erzeugt, so wird dieses umgehend implementiert und nach einem Neustart aktiv.<br>Wird ein CSR erstellt, so erscheint unten im **SSL** Menü die Schaltfläche **Download and Import signed Certificate...**. Diese Führt zum Folgemenü **Download and Import signed Certificate** 183 welches den CSR zur weiterleitung an die CA. |

Über die Schaltfläche **Create Request** - ganz unten im Menü - wird die unter **Signature** gewählte Aktion gestartet.

### Sektion Upload existing key

Ist bereits ein SSL-Zertifikat vorhanden, so kann dieses auf zwei Arten - abhängig vom vorliegenden Zertifikats-Format (pem oder PKCS#12 also p12 oder pfx) - hochgeladen werden.
Dabei werden die ersten beiden Parameter ausschliesslich für die Integration des pem-Formats, die beiden letzteren Parameter für die Integration des PKCS#12-Formates benötigt.

| Parameter | Beschreibung |
|---|---|
| X.509 Key<br>Note: Remove password before uploading a key | In dieses Feld wird der Private Schlüssel aus der pem-Datei eingefügt. Hierfür wird die pem-Datei mit einem Editor geöffnet. Falls der Private Schlüssel durch ein Kennwort geschützt ist, muss dieses zuvor entfernt werden. Im Anschluss wird der Private Schlüssel (dieser beginnt mit -----BEGIN PRIVATE KEY----- und endet mit -----END PRIVATE KEY-----) in das Eingabefeld kopiert.<br>**Die Eingabe muss unbedingt mit einer Leerzeile abgeschlossen werden!** |
| X.509 Certificate (and optional intermediate certificates) | In dieses Feld wird der Öffentliche Schlüssel aus der pem-Datei eingefügt. Dieser ist unterhalb des Privaten Schlüssel in der pem-Datei zu finden und beginnt mit -----BEGIN CERTIFICATE----- und endet mit -----END CERTIFICATE-----.<br>Unter Umständen sind in der pem-Datei weitere Zertifikate enthalten. Dabei handelt es sich um Zwischen- oder auch Intermediate- Zertifikate, welche unterhalb des Öffentlichen Schlüssels in dieses Feld kopiert werden müssen. Zuletzt wird das Zertifikat der Root CA eingefügt.<br>**Die Eingabe muss unbedingt mit einer Leerzeile abgeschlossen werden!**<br><br>**Hinweis:**<br>**In dieses Eingabefeld sollten alle notwendigen Zwischenzertifikate für eine vollständige Zertifikatskette eingefügt werden. Eine unvollständige Zertifikatskette führt bei der Zertifikatsprüfung immer dann zu Problemen, wenn der Gegenstelle diese nicht bereits bekannt ist. Internet-Tools - wie zum Beispiel CheckTLS** |

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| | **- zeigen dann einen falschen TLS-Status an.<br>Nicht jede pem-Datei enthält die komplette Zertifikatskette. In diesem Fall müssen die benötigten Zwischenzertifikate gegebenenfalls anderweitig besorgt werden.** |
| **Key and certificate in PKCS12 format** | Über die Internet-Browser Schaltfläche "Datei auswählen" wird die PKCS#12-Datei (diese hat die Endung .p12 oder .pfx) ausgewählt.<br> <br>**Hinweis:<br>Auch hier muss darauf geachtet werden, dass diese Datei die komplette Zertifikatskette, also auch die Zwischenzertifikate enthält. Gegebenenfalls kann nach dem Import der PKCS#12 Datei ein Backup des Zertifikates (siehe SSL 179) vorgenommen werden. Die dadurch zur Verfügung stehende pem-Datei kann mit einem Editor geöffnet und anschliessend wie oben beschrieben wieder inklusive Zwischenzertifikate importiert werden.** |
| PKCS12 password | Nachdem eine PKCS#12-Datei den Privaten Schlüssel enthält, ist diese Passwort geschützt. Das Passwort muss vor dem Import der oben ausgewählten PKCS#12-Datei in dieses Eingabefeld eingegeben werden. |

Über die Schaltfläche **Upload Key and Certificate** wird das SSL-Zertifikat in die Appliance hochgeladen.
Aktiv wird das Zertifikat nach einem Neustart der Appliance.

#### 7.7.1.1 Untermenü Download and Import signed Certificate

**Sektion Request**

Das Eingabefeld enthält den CSR wie er an die CA übermittelt werden muss. Die geschieht häufig über ein Texteingabefeld auf der Webseite der CA.

**Sektion Import Certificate**

Wird nach dem Hochladen des CSR zur CA von dieser das Zertifikat zurückgeliefert, so ist der Inhalt dieses Zertifikats in dieses Eingabefeld einzugeben.
Diese Zertifikat beginnt mit -----BEGIN CERTIFICATE----- und endet mit -----END CERTIFICATE-----.
Unter Umständen werden von der CA weitere Zertifikate zur Verfügung gestellt. Dabei handelt es sich um Zwischenzertifikate, welche unterhalb des Öffentlichen Schlüssels in dieses Feld kopiert werden müssen.
**Die Eingabe muss unbedingt mit einer Leerzeile abgeschlossen werden!**

**Hinweis:
In dieses Eingabefeld sollten alle notwendigen Zwischenzertifikate für eine vollständige Zertifikatskette eingefügt werden. Eine unvollständige Zertifikatskette führt bei der Zertifikatsprüfung immer dann zu Problemen, wenn der Gegenstelle diese nicht bereits bekannt ist. Internet-Tools - wie zum Beispiel CheckTLS - zeigen dann einen falschen TLS-Status an.
Nicht jede CA liefert automatisch die komplette Zertifikatskette. In diesem Fall müssen die benötigten Zwischenzertifikate gegebenenfalls anderweitig**

© 2015 SEPPmail AG

**besorgt werden.**

Über die Schaltfläche **Import Certificate** wird der Vorgang abgeschlossen. Im Anschluss muss die Appliance neu gestartet werden.das SSL-Zertifikat in die Appliance hochgeladen.

Die Schaltfläche **Cancel this Certificate enrollmant process** bricht den Vorgang ab. Nach dem Abbruch besteht keine Möglichkeit mehr das zum CSR passende Zertifikat einzubinden!
Die Appliance kann durch schlichten Wechsel in ein anderes Menü weiter konfiguriert werden, ohne den Vorgang abzubrechen.

© 2015 SEPPmail AG

## 7.8 CA

Die SEPPmail-Appliance beinhaltet eine vollständige CA. Diese kann als Self-Signed-CA aber auch als Sub-CA konfiguriert werden. Alternativ können Trusted-CA Zertifikate automatisiert über die Managed Public Key Infrastructure (MPKI) Connectoren bezogen werden.
Die Verwendung einer Self-Signed-CA ist an dieser Stelle ausser für Testzwecke nicht zu empfehlen, da die Signatur von mit Self-Signed-Zertifikaten signierten E-Mails in der Regel vom Empfänger nicht automatisiert geprüft werden kann.

**Sektion Issued To**

Diese Sektion zeigt Informationen über den Inhaber des CA-Zertifikates.
Abhängig vom Zertifikat müssen nicht alle hier aufgeführten Parameter vorhanden sein.

| Parameter | Beschreibung |
|---|---|
| **Name (CN)** | Gibt den Namen der eigenen CA an |
| **E-Mail Address** | In der Regel der wird die E-Mail-Adresse des Verwalters der eigenen CA oder dessen Abteilung eingetragen. |
| **Org. Unit (OU)** | Organisationseinheit wie zum Beispiel ein Abteilungsname wie "Sicherheit" |
| **Organization (O)** | Gibt die Organisation an, für welche das Zertifikat ausgestellt wurde, zum Beispiel "Firma" |
| **Locality (L)** | Standort zum Beispiel eine Stadt wie "Neuenhof" |
| **State (ST)** | Bundesland, Kanton, Provinz oder Ähnliches, zum Beispiel "AR" für "Appenzell Ausserrhoden" |
| **Country (C)** | Land, zum Beispiel "CH" für "Schweiz" |
| **Serial No.** | Seriennummer des Zertifikats |

**Sektion Issued By**

Diese Sektion zeigt Informationen über den Aussteller des CA-Zertifikates (Root-Zertifikat).
Abhängig vom Aussteller müssen nicht alle hier aufgeführten Parameter vorhanden sein.

| Parameter | Beschreibung |
|---|---|
| **Name (CN)** | Name der ausstellenden CA |
| **E-Mail Address** | In der Regel eine E-Mail-Adresse für Supportanfragen an den Aussteller |
| **Org. Unit (OU)** | Gibt eine Organisationseinheit des Ausstellers an |
| **Organization (O)** | Gibt die ausstellende Organisation an |

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| **Locality (L)** | Gibt den Standort des Ausstellers an |
| **State (ST)** | Gibt ein Bundesland, Kanton, Provinz oder Ähnliches des Ausstellers an |
| **Country (C)** | Gibt das Land des Ausstellers an |

### Sektion Validity

Gibt die Gültigkeit des eigenen CA-Zertifikates an.

| Parameter | Beschreibung |
|---|---|
| **Issued on** | Ausstelldatum des Zertifikates |
| **Expires on** | Ablaufdatum des Zertifikates |

### Sektion Fingerprint

Gibt den Hash des eigenen CA-Zertifikates an.

| Parameter | Beschreibung |
|---|---|
| **Hashalgorhytmus des Zertifikates, zum Beispiel SHA1** | Der Fingerprint dient zur Überprüfung eines Zertifikats. Beispiel eines SHA1 Fingerprints:<br>48:2D:99:B1:64:C1:14:9C:B3:F2:C0:8D:FA:7F:40:9F:22:F5:11:F5 |

### Sektion Certificate Revocation List

Wurde die interne CA konfiguriert, so hält diese eine Revocation List für die von ihr ausgestellten Zertifikate vor. Sollte ein Privater Schlüssel kompromittiert worden sein, so kann dieser in der Benutzerkonfiguration (siehe **Benutzerdetails** 204) als ungiltig erklärt werden und taucht dann in der Revocation List auf. Diese kann über die Schaltfläche **Create and Download CRL** heruntergeladen und somit abgefragt werden.

### Sektion Internal CA Settings

In dieser Sektion werden die Einstellungen für die Self-Signed- beziehungsweise Sub-CA eingegeben. Die genannten Extension Settings sind die Standard Einstellung bei Einrichtung einer Self-Signed-CA. Soll eine Sub-CA Eingerichtet werden, gibt in der Regel der Betreiber der Haupt-CA entsprechende Werte vor.

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| Static Subject Part | Als "Static Subject Part" tauchen im Standard die bei der CA Erstellung eingegebenen Parameter für Land, Organisationseinheit und Organisation auf, also zum Beispiel<br>/C=CH/OU=Sicherheit/O=Firma |
| Validity in days | Gibt die Gültigkeit der ausgestellten Zertifikate in Tagen an.<br> <br>**Hinweis:**<br>**Diese Einstellung gilt auch für die von der Appliance generierten openPGP Schlüsselpaare** |
| Automatically renew expiring certificates if validity days left less than | Gibt an, ob und wenn wieviele Tage vor dem Ablaufen ein Zertifikat erneuert werden soll. Je früher vor Ablauf dieses erneuert wird, desto mehr Verbreitung wird das neue Zertifikat über die E-Mail Signatur bis zum Ablaufen des Vorgänger-Zertifikates finden. Dadurch steht das neue Zertifikat zuverlässiger für Kommunikationspartner zur Verschlüsselung bereit.<br> <br>**Hinweis:**<br>**Zertifikate werden nur für diejenigen Benutzer neu generiert, welche auch aktiv sind.**<br>**Das heisst, sendet ein Benutzer innerhalb des angegebenen Zeitraums** validity days left **keine E-Mail, so wird auch kein neues Zertifikat generiert.**<br> <br>**Hinweis:**<br>**Diese Einstellung gilt auch für die von der Appliance generierten openPGP Schlüsselpaare** |

| | | | | |
|---|---|---|---|---|
| **Extension setting** | name: | authorityKeyIdentifier | value: | keyid,issuer:always |
| | Fügt den durch diese CA ausgestellten Zertifikaten die über den Wert (value:) angegebenen Informationen über die ausstellende CA hinzu | | **keyid**: subjectKeyIdentifier (siehe nächste Option)<br>**issuer**: IssuerName, Serialnumber<br>**:always**: Gibt eine Fehlermeldung aus, wenn das Kopieren der angegebenen Optionen fehlschlägt | |
| **Extension setting** | name: | subjectKeyIdentifier | value: | hash |
| | Gibt die Art des Fingerprints des ausgestellten Zertifikats an | | **hash**: bildet einen Hash-Wert gemäss RFC 3280<br>**hex**: Ein vordefinierter Hex-Wert wird dem Zertifikat angehängt (nicht empfohlen!) | |
| **Extension setting** | name: | subjectAltName | value: | email:copy |
| | Ermöglicht das Einbinden weiterer Alternativnamen in das ausgestellte Zertifikat. | | **email**: E-Mail-Adresse<br>***copy****: fügt automatisch eine Kopie der E-Mail-Adresse aus dem "SubjectName" hinzu*<br>**URI**: uniform resource indicator<br>**DNS**: DNS domain name<br>**RID**: registered ID: OBJECT IDENTIFIER<br>**IP**: IP-Adress im v4 oder v6 Format<br>**dirName**: sollte auf einen distinguished name (DN) | |

© 2015 SEPPmail AG

| Parameter | Beschreibung | | | |
|---|---|---|---|---|
| | | | zeigen. Mehrfach eingabe durch + möglich. | |
| **Extension setting** | name: | basicConstraints | value: | CA:FALSE |
| | Zeigt auf, ob es sich bei dem Ausgestellten Zertifikat um ein CA Zertifikat handelt. | | **CA**: mögliche Werte sind TRUE oder FALSE<br>**pathlen**: optional bei CA:TRUE: gibt die maximale Anzahl von CAs an, welche | |
| **Extension setting** | name: | nsComment | value: | OpenSSL Generated Certificate |
| | Kommentareintrag für das Zertifikat | | Frei wählbarer Kommentar | |
| **Extension setting** | name: | nsCertType | value: | client, email |
| | Gibt den Zertifikatstyp an (Netscape) | | **client, server, email, objsign, reserved, sslCA, emailCA, objCA** | |
| **Extension setting** | name: | keyUsage | value: | nonRepudiation, digitalSignature, keyEncipherment |
| | Gibt den/die erlaubten Verwendungszweck(e) für das Zertifikat an. | | **digitalSignature**: Digitale Signatur<br>**nonRepudiation**: Nachweisbarkeit<br>**keyEncipherment**: Schlüssel Verschlüsselung<br>**dataEncipherment**: Datenverschlüsselung<br>**keyAgreement**: Schlüsselvereinbarung<br>**keyCertSign**: Zertifikatssignatur<br>**cRLSign**: Revocation List Signatur<br>**encipherOnly**: nur Verschlüsselung<br>**decipherOnly**: nur Entschlüsselung | |
| **(Extension setting)** | name: | crlDistributionPoints | value: | URI:https://<IhreCA>/certs.crl |
| | Fügt den Pfad zur Revocation List der CA an das Zertifikat an. (diese Einstellung muss bei Bedarf manuell hinzugefügt werden) | | **URI**: Pfad zur Revocation List. Mehrere URLs werden kommagetrennt eingegeben. | |
| **New Extension** | name: | | value: | |
| | An dieser Stelle können bei Bedarf weitere Einstellungen vorgenommen werden. Nach dem Speichern einer weiteren Extension kommt erscheint jeweils eine weitere Eingabezeile. | | | |

**Sektion External CA**

An dieser Stelle wird die Entscheidung getroffen ob, und wenn welche CA für den (teil-)automatischen Bezug von Trusted-CA-Zertifikaten zur Verfügung gestellt werden soll.

**Hinweis:**
**Wird das automatische Erneuern von Zertifikate in den MPKI Einstellungen aktiviert, so werden nur für diejenigen Benutzer neue Zertifikate generiert, welche auch aktiv sind.**
**Das heisst, sendet ein Benutzer innerhalb des angegebenen Zeitraums** validity days left **keine E-Mail, so wird auch kein neues Zertifikat generiert.**

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| **Select MPKI** | ○ A-Trust<br>○ D-Trust<br>○ none<br>○ S-Trust<br>○ SwissSign<br>Über die Schaltfläche **Save** wird die Auswahl gesichert. |
| **Configure MPKI** | Dieser Parameter taucht nur auf, wenn eine CA ausgewählt wurde -also nicht "none".<br>Über die Schaltfläche **<Ausgewählte CA> connector...** wird dann der Zugang und die Parameter für die Schnittstelle konfiguriert. Die entsprechenden Konfigurationsdaten stellt der CA Anbieter zur Verfügung. |

Über die Schaltflächen **Download Certificate** kann das Root CA Zertifikat - also der Öffentliche Schlüssel - der CA heruntergeladen werden. Dieser kann gegebenenfalls einem Kommunikationspartner zur Verfügung gestellt werden, damit dieser Signaturen von E-Mails welche mit Zertifikaten Ihrer Self-Signed-CA signiert wurden automatisiert prüfen kann.
Über **Download Key** kann der Private Schlüssel heruntergeladen und somit gesichert werden.

Die Schaltfläche **Request a new Certificate...** führt zum Untermenü **Request a new Certificate** 181 - wie es bereits aus dem Menü SSL bekannt ist - über welches die CA als Self-signed- oder Sub-CA eingerichtet wird.

© 2015 SEPPmail AG

## 7.9 Administration

Dieses Menü beinhaltet Funktionen zur Verwaltung des Systems.

### Sektion License and Registration

Ist eine Gültige Lizenz vorhanden, so wird in diesem Abschnitt die Meldung "Valid License detected" ausgegeben.
Andernfalls muss an dieser Stelle die Registrierung der Appliance vorgenommen werden. im Normalfall geschieht das über die Schaltfläche **Register this device...**, welche das Untermenü **Register this device** 193 öffnet.
Ist der Zugang zum SEPPmail-Lizenzserver (update.seppmail.ch beziehungsweise support.seppmail.ch) über TCP Port 22 (siehe **Firewall / Router einrichten** 63 sowie Sektion **Proxy Settings** des Menüpunktes **System** 119) nicht möglich, da es sich zum Beispiel um ein PCI gehärtetes oder ein DMZ abgeschottetes System handelt, so kann die Registrierung über **Import License File...** vorgenommen werden.

### Sektion Update

Über die Schaltfläche **Check for Update** wird die komplette Versions-Historie sowie Inhalte verfügbarer und geplanter Updates der SEPPmail-Appliance ngezeigt. Sollten bei einem Update Nacharbeiten - in seltenen Fällen muss zum Beispiel das Ruleset neu generiert werden - notwendig sein, so ist auch dies in roter Schrift zu sehen.
Weiterhin kann durch klicken dieser Schaltfläche ein Abgleich mit dem SEPPmail-Lizenzserver erzwungen werden, wodurch zum Beispiel kurzfristig angeforderte Lizenzänderungen sofort übernommen werden.

**Fetch Update** startet bei verfügbarem Update den Download der Firmware vom SEPPmail-Updateserver und startet das System im Anschluss mit der neuen Firmware. Durch erneutes Klicken dieser Schaltfläche während des Downloads wird jeweils der Fortschritt in % ausgegeben.
**Prefetch (reboot manually)** startet bei verfügbarem Update den Download der Firmware vom SEPPmail-Updateserver. Diese wird beim nächsten manuellen Reboot übernommen.
Ist der Zugang zum SEPPmail-Lizenzserver (update.seppmail.ch beziehungsweise support.seppmail.ch) über TCP Port 22 (siehe **Firewall / Router einrichten** 63 sowie Sektion **Proxy Settings** des Menüpunktes **System** 119) nicht möglich, da es sich zum Beispiel um ein PCI gehärtetes oder ein DMZ abgeschottetes System handelt, so kann eine Update Datei über den Support angefordert werden. Diese Datei wird über **Upload** hochgeladen. Durch einem Neustart der SEPPmail-Appliance wird die neue Firmware aktiv.

**Hinweis:**
In der Regel wird immer die aktuellste Firmware eingespielt. In seltenen Fällen ist jedoch das Update in mehreren Schritten notwendig, wenn zum Beispiel Abhängigkeiten bei den Konfigurationsdateien bestehen. In diesem Fall muss die Appliance so oft aktualisiert werden, bis Sie auf dem aktuellen Stand ist (Meldung "**You already have the latest version installed** ").

### Sektion Backup

Die Schaltfläche **Download** startet das Herunterladen der Backup-Datei. Diese Datei beinhaltet ausschliesslich Konfiguration und Schlüsselmaterial der SEPPmail-Appliance. Voraussetzung für den Download des Backups ist die Vergabe eines Backup Passwortes, welches via **Change Password** gesetzt beziehungsweise geändert werden kann.
Soll ein Backup in die Appliance zurückgespielt werden, so erfolgt dies durch klicken von **Import Backup File...**. Hierfür wird das zum Zeitpunkt der Erstellung des Backups gültige Backup-Passwort

© 2015 SEPPmail AG

benötigt.

**Hinweis:**
Mitglieder der Gruppe "backup" (siehe Groups 213 Sektion backup (Backup Operator)) erhalten täglich die Sicherungsdatei per E-Mail zugesandt. Voraussetzung ist natürlich ein gesetztes Backup Passwort.

### Sektion System

Reboot... startet das System neu. Es erscheint ein Dialog zur Eingabe eines Sicherheitscodes, wodurch ein versehentlicher Neustart verhindert wird.
Shut down... fährt das System herunter. Es erscheint ein Dialog zur Eingabe eines Sicherheitscodes, wodurch ein versehentliches Herunterfahren verhindert wird.

### Sektion Database and System Settings

Perform factory reset... setzt das System auf Werkszustand zurück. Es erscheint ein Dialog zur Eingabe eines Sicherheitscodes in umgekehrter Schreibweise um ein ungewolltes Zurücksetzen zu verhindern.

### Sektion Import

In dieser Sektion werden zahlreiche (Massen-)Importfunktionen zur Verfügung gestellt.

| Parameter | Beschreibung |
|---|---|
| **Import Users (CSV)** | Über die Schaltfläche Import können Encryption/Signature-Benutzer mittels csv-Datei mit dem Aufbau "USERID;NAME;EMAIL;PASSWORD" importiert werden. Dabei ist die Vergabe eines Passwortes optional (siehe Users 203). Bei Benutzern, welche durch die SEPPmail-Appliance automatisch generiert wurden entsprechen USERID;NAME;EMAIL jeweils der E-Mail-Adresse des Benutzers, was die Einmaligkeit garantiert. |
| **Import GINA Users (CSV)** | Über die Schaltfläche Import können GINA-Benutzer mittels csv-Datei mit dem Aufbau "EMAIL;PASSWORD;NAME;MOBILE" importiert werden. Die Angabe einer Mobilfunk-Nummer ist dabei optional.<br>Denkbar wäre die Eingabe einer Kundenliste deren jeweiliges Initialpasswort die Postleitzahl ist.<br>Erfolgt bei mandantenfähigen Systemen der Import durch den Mandanten-Admin, so werden die mittels dieser Funktion importierten GINA-Benutzer automatisch dem entsprechenden Mandanten zugeordnet. |
| **Import openPGP secret keys** | Über die Schaltfläche Import openPGP secret keys ist das Importieren privater openPGP Schlüssel möglich. Sollte für die im Schlüssel vorhandene E-Mail-Adresse noch kein Benutzer auf der SEPPmail-Appliance vorhanden sein, so wird dieser automatisch durch diese Aktion angelegt.<br>Der Import ist sowohl über eine Datei, als auch durch Einfügen als Text möglich jeweils unter Angabe der passenden Passphrase möglich.<br>Durch das Aneinanderreihen von Schlüsseln - egal ob als Datei oder als Text - ist auch ein Massenimport möglich. Dies setzt allerdings voraus, dass alle Schlüssel die selbe Passphrase haben. |
| **Import S/MIME keys** | Über die Schaltfläche Import S/MIME keys ist das Importieren von PKCS#12 Dateien (diese haben die Endung .p12 oder .pfx), welche den privaten S/MIME- |

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| | Schlüssel enthalten, unter Angabe der passenden Passphrase möglich. Sollte für die im Schlüssel vorhandene E-Mail-Adresse noch kein Benutzer auf der SEPPmail-Appliance vorhanden sein, so wird dieser automatisch durch diese Aktion angelegt.<br>Der Import ist sowohl über eine Datei, als auch durch Einfügen als Text möglich jeweils unter Angabe der passenden Passphrase möglich.<br>Durch das packen mehrer PKCS#12 Dateien in eine unverschlüsselte ZIP-Datei ohne Ordnerstruktur ist auch ein Massenimport möglich. Dies setzt allerdings voraus, dass alle Schlüssel die selbe Passphrase haben. |
| **Import S/MIME certificates** | Über **Import S/MIME user and/or CA certificates** können öffentliche S/MIME Schlüssel zur Verschlüsselung an Kommunikationspartner, wie auch CA Zertifikate für die automatische S/MIME Signaturprüfung importiert werden. Durch das packen mehrerer Schlüssel Dateien in eine unverschlüsselte ZIP-Datei ohne Ordnerstruktur ist auch hier ein Massenimport möglich. |

**Sektion Establish Support Connection**

Sollten auf der SEPPmail-Appliance unerwartet Probleme auftauchen, so kann mittels **Connect** eine Support Verbindung zum Hersteller aufgebaut werden. Hierdurch wird eine SSH Verbindung (TCP Port 22) zum SEPPmail-Supportserver aufgebaut.

© 2015 SEPPmail AG

### 7.9.1 Untermenü Register this device

Die Registrierungsdaten sollten sorgfältig ausgefüllt werden, da unter anderen bei CERT-Meldungen, von welchen die SEPPmail-Appliance betroffen ist, die hier genannten Kontakte bei Bedarf informiert werden.
Werden mehrere Appliances für den selben Kunden registriert, so ist darauf zu achten, dass die Eingaben identisch gemacht werden.

**Sektion Customer Information**

Eingabefeld für die Kundendaten.

| Parameter | Beschreibung |
|---|---|
| Company | Pflichtfeld. Firmenname des Kunden. |
| Address 1 | Pflichtfeld. Adresse des Kunden. |
| Address 2 | Optional. Zusätzliches Adressfeld. |
| City | Pflichtfeld. Stadt des Kunden. |
| Postal Code | Pflichtfeld. Postleitzahl des Kunden. |
| Country | Pflichtfeld. Land des Kunden. |
| First Name | Pflichtfeld. Vorname des Ansprechpartners beziehungsweise der zuständigen Abteilung beim Kunden. |
| Last Name | Pflichtfeld. Nachname des Ansprechpartners beziehungsweise der zuständigen Abteilung beim Kunden. |
| Email Address | Pflichtfeld. E-Mail-Adresse des Ansprechpartners beziehungsweise der zuständigen Abteilung beim Kunden. |
| Phone Number | Pflichtfeld. Telefonnummer in der Form "+<Ländercode> <Vorwahl ohne null"0"> <Rufnummer inklusive Durchwahl>" des Ansprechpartners beziehungsweise der zuständigen Abteilung beim Kunden. |
| Mobile Phone Number | Optional. Mobilfunknummer in der Form "+<Ländercode> <Vorwahl ohne null"0"> <Rufnummer inklusive Durchwahl>" des Ansprechpartners beziehungsweise der zuständigen Abteilung beim Kunden. |

**Sektion Reseller Information**

Eingabefeld für die Daten des SEPPmail-Partners

| Parameter | Beschreibung |
|---|---|
| Company | Pflichtfeld. Firmenname des Partners. |
| Address 1 | Pflichtfeld. Adresse des Partners. |

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| Address 2 | Optional. Zusätzliches Adressfeld. |
| City | Pflichtfeld. Stadt des Partners. |
| Postal Code | Pflichtfeld. Postleitzahl des Partners. |
| Country | Pflichtfeld. Land des Partners. |
| First Name | Pflichtfeld. Vorname des Ansprechpartners beziehungsweise der zuständigen Abteilung beim Partners. |
| Last Name | Pflichtfeld. Nachname des Ansprechpartners beziehungsweise der zuständigen Abteilung beim Partners. |
| Email Address | Pflichtfeld. E-Mail-Adresse des Ansprechpartners beziehungsweise der zuständigen Abteilung beim Partners. |
| Phone Number | Pflichtfeld. Telefonnummer in der Form "+<Ländercode> <Vorwahl ohne null"0"> <Rufnummer inklusive Durchwahl>" des Ansprechpartners beziehungsweise der zuständigen Abteilung Partners. |
| Mobile Phone Number | Optional. Mobilfunknummer in der Form "+<Ländercode> <Vorwahl ohne null"0"> <Rufnummer inklusive Durchwahl>" des Ansprechpartners beziehungsweise der zuständigen Abteilung Partners. |

**Sektion Activation Code**

| Parameter | Beschreibung |
|---|---|
| Enter the device ID of this virtual appliance from your license document. Leave empty to get a test license | Ist bereits das "SEPPmail License Certificate" der Kauflizenz vorhanden, so ist die darauf befindliche "Device-ID" in dieses Feld in der Form XXXX-XXXX-XXXX einzutragen. Somit werden die erworbenen Lizenzen auf die Appliance übertragen. Wird dieses Feld leer gelassen, so zieht die Appliance automatisch eine 30-tägige Testlizenz.<br><br>**Hinweis:**<br>Wurde eine Testlizenz bezogen und soll diese im Anschluss in die Produktion übernommen werden, so ist bei der Bestellung unbedingt die "Device ID" aus der Sektion System des Menüs Home (siehe Home 116) mit anzugeben.<br><br>**Hinweis:**<br>Wurde die "Device-ID" eines "SEPPmail License Certificate" bereits einmal verwendet, so lässt sich dieses - zum Beispiel nach einer Neuinstallation - kein zweites mal Verwenden. In diesem Fall ist der Support zu kontaktieren. |

Über das klicken der Schaltfläche Send wird der Registrierungsprozess abgeschlossen.

© 2015 SEPPmail AG

## 7.10 Cluster

Dieses Menü bietet die Möglichkeit mehrere Appliances zu einem Cluster zusammen zu fügen.
Das Verhalten des Clusters ist dabei stark von den vorgenommenen Systemeinstellungen (siehe unter Anderem Menü System 119 Sektionen IP ALIAS Addresses und SMTP Loadbalancer) Maschinen, welche dem Cluster hinzugefügt werden übernehmen die Einstellungen der Basis-Maschine. Das heisst alle eventuell bereits vorgenommenen Einstellungen werden überschrieben. Ausgenommen vom Clustering bleiben die Menüpunkte, welche maschinenbezogene Daten enthalten, wie **System**, **SSL**, **CA**, **Logs** und **Statistics**.

### Sektion Prepare for Cluster

Über die Schaltfläche **Download Cluster Identifier** wird das Zertifikat für die Herstellung der SSH Verbindung vom zukünftigen Cluster Partner zur Basis-Maschine heruntergeladen. In der Regel heisst diese Datei "clusterid.txt". Das heisst diese Aktion wird an der Maschine vorgenommen, von welcher die Einstellungen übernommen werden sollen.

### Sektion Add this device to existing cluster

Diese Sektion erscheint nur dann, wenn die SEPPmail-Appliance nicht bereits in einem Cluster Verbund integriert ist und dient dem Hinzufügen zu einem Cluster.

**Achtung:**
Alle Einstellungen, welche nicht maschinenbezogen sind (siehe Sektion Prepare for Cluster), werden durch diese Aktion mit den Einstellungen der Basis-Maschine überschrieben. Sollten Unsicherheiten bezüglich der Aktion bestehen, empfiehlt sich dringend zuvor ein manuelles Backup zu erstellen (siehe Administration 190 Sektion Backup).

| Parameter | Beschreibung |
|---|---|
| Cluster Identifier | Über die Browserschaltfläche "Datei auswählen" wird das für die SSH Verbindung benötigte Zertifikat der Basis-Maschine "clusterid.txt" (siehe Sektion Prepare for Cluster) ausgewählt. |
| Cluster Member IP | An dieser Stelle wird die physikalische IP-Adresse (kein Alias!, also virtuelle Adresse) der Basis-Maschine über welche die Cluster Kommunikation stattfinden soll sowie der zu verwendende Port (im Standard Port 22 für das SSH-Protokoll) angegeben. |
| IP address of this device | An dieser Stelle wird die physikalische IP-Adresse (kein Alias!, also virtuelle Adresse, siehe System 119 Sektion IP Addresses) dieser Maschine über welche die Cluster Kommunikation stattfinden soll sowie der zu verwendende Port (muss identisch mit dem unter Cluster Member IP eingegebenen sein) angegeben. |
| **Connect** | Über die Schaltfläche **Start** wird die Maschine dem Cluster hinzugefügt. |

### Sektion cluster members

Diese Sektion erscheint nur dann, wenn die SEPPmail-Appliance bereits Bestandteil eines Cluster ist. In diesem Fall werden alle Clusterpartner mit den folgenden Daten gelistet:

© 2015 SEPPmail AG

| Spalte | Beschreibung |
|---|---|
| **Device ID** | Zeigt die "Device ID" des jeweiligen Cluster Partners an.<br>Das Entfernen eines entfernten Cluster Partners kann durch klicken auf die "Device ID" erfolgen. Hierdurch öffnet ein weiteres Menü, in welchem dann der Server über die Schaltfläche **Remove device from cluster** entfernt werden kann. Die Datenbank bleibt mit dem zuletzt synchronisierten Stand auf dem entfernten System erhalten.<br>Das Entfernen der lokalen Maschine aus dem Cluster Verbund erfolgt wie in Sektion **Remove from cluster** beschrieben. |
| **IP Address** | Zeigt die "IP Adresse" des jeweiligen Cluster Partners an, welche für die Cluster Kommunikation konfiguriert wurde. |
| **Port** | Zeigt den Kommunikations-Port an (im Standard Port 22 für das SSH-Protokoll) |
| **Status** | Arbeitet der Cluster korrekt, so steht hier<br>"OK (XXXX entries in remote database, XXXX entries in local Database)"<br>wobei die Anzahl "XXXX" identisch sein sollte. |
| **Comment** | Zeigt den für den Clusterpartner definierten Kommentar an (siehe **System** 119 "Advanced View" Sektion **Comment**) |
| **Location** | Zeigt den für den Clusterpartner definierten Standort an (siehe **System** 119 "Advanced View" Sektion **Comment**) |

### Sektion Remove from cluster

Durch klicken der Schaltfläche **remove this device from cluster** wird die Maschine aus dem Cluster herausgenommen. Die lokale Datenbank bleibt dabei erhalten und hat den Stand der letzten Synchronisierung im Cluster.

### Sektion Add this device as frontend server (no local database)

Diese Sektion erscheint nur dann, wenn die SEPPmail-Appliance nicht bereits in einem Cluster Verbund integriert ist und dient dem Hinzufügen der Maschine als Frontend Server zu einer anderen Maschine oder einem Cluster. Als Frontend Server wird ein Cluster Partner ohne lokale Datenbank bezeichnet.
Sollte aufgrund von Revisionsvorgaben die SEPPmail-Appliance in einer DMZ platziert werden müssen, in welcher keine Datenhaltung - in diesem Fall in erster Linie Schlüsselmaterial - erlaubt ist, so kann über diese Funktion eine Trennung zwischen dem Datenbanksystem (Backend) und dem E-Mail verarbeitenden System (Frontend) vollzogen werden.
Der Frontend Server erhält in diesem Fall jeweils nur die diejenigen Daten vom Backend Server, welche aktuell zur Verarbeitung einer E-Mail benötigt werden. Der Backend Server steht ausserhalb der DMZ und hält die Daten in seiner Datenbank.
Frontend Server werden nicht in der Sektion **cluster members** der Backend Systeme angezeigt.

| Parameter | Beschreibung |
|---|---|
| Cluster Identifier | Über die Browserschaltfläche "Datei auswählen" wird das für die SSH Verbindung benötigte Zertifikat der Basis-Maschine "clusterid.txt" (siehe Sektion **Prepare for Cluster**) ausgewählt. |

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| Existing Appliance IP | An dieser Stelle wird IP-Adresse der "Backend Maschine" über welche die Cluster Kommunikation stattfinden soll sowie der zu verwendende Port (im Standard Port 22 für das SSH-Protokoll) angegeben.<br>Existiert ein "Backend Cluster", so kann an dieser Stelle eine virtuelle IP-Adresse (siehe System 119 Sektion IP ALIAS Addresses) verwendet werden. Es besteht aber auch die Möglichkeit, der "Frontend Maschine" weitere Backend Server im Nachhinein hinzu zu fügen (siehe Sektion Add additional Backend) falls keine virtuelle IP-Adresse verfügbar ist. |
| **Connect** | Über die Schaltfläche Start wird die Maschine dem Cluster hinzugefügt. |

### Sektion Remote LDAP Server

Diese Sektion erscheint nur dann, wenn die SEPPmail-Appliance als Frontend Server bereits Bestandteil eines Cluster ist. In diesem Fall werden alle Backend Server mit den folgenden Daten gelistet:

| Spalte | Beschreibung |
|---|---|
| **IP Address** | Zeigt die "IP Adresse" der jeweiligen LDAP-(Backend-)Maschine an.<br>Das Entfernen eines LDAP-(Backend-)Servers erfolgt durch klicken auf die IP-Adresse. Hierdurch öffnet ein weiteres Menü, in welchem dann der Server über die Schaltfläche Remove device from cluster entfernt werden kann.<br>Das Entfernen der lokalen Maschine als Frontend Server erfolgt wie in Sektion Detach from LDAP Server beschrieben. |
| **Port** | Zeigt den Kommunikations-Port an (im Standard Port 22 für das SSH-Protokoll) |
| **Status** | Arbeitet der Cluster korrekt, so steht hier<br>"OK (XXXX entries in remote database)" |

### Sektion Detach from LDAP Server

Über die Schaltfläche Detach wird die SEPPmail-Appliance als Frontend Server entfernt. Dabei wird eine leere Lokale Datenbank auf dem System angelegt.

### Sektion Add additional Backend

Sollen mehrere Backend Server aus einem Backend Cluster für LDAP-Anfragen herangezogen werden, ohne dass eine virtuelle IP-Adresse zur Verfügung steht, so können diese über diese Option eingebunden werden.

| Parameter | Beschreibung |
|---|---|
| Existing Appliance IP | An dieser Stelle wird die physikalische IP-Adresse einer weiteren Backend Maschine sowie der zu verwendende Port (im Standard Port 22 für das SSH-Protokoll) angegeben.<br>Hierdurch kann ein Backend Cluster ohne Verwendung von virtuellen IP- |

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| | Adressen zur Verfügung stehen. |
| **Connect** | Über die Schaltfläche **Start** wird die zusätzliche Backend Maschine hinzugefügt. |

© 2015 SEPPmail AG

## 7.11 Logs

Dieses Menü stellt Logs für unterschiedliche Komponenten zur Verfügung

**Sektion Other Logs**

Sofern die GINA-Technologie nicht deaktiviert wurde (siehe **Mail Processing** 147 Sektion **Ruleset Generator** **Advanced Options "**Completely disable GINA technology**"**) wird eine entsprechende Log-Datei geführt, welche über die Schaltfläche **Show GINA log...** einzusehen ist.
Bei lizensiertem Protection Pack und aktiviertem Black- Greylisting (siehe **Mail System** 129 Sektionen **Antispam**, **Blacklists** und **Manual Blacklisting / Whitelisting**) werden diese Vorgänge in einer entsprechenden Log-Datei geführt. Diese Log-Datei kann über die Schaltfläche **Show Blacklist / Gereylist Log...** eingesehen werden.

**Sektion Queue Control**

Sofern die E-Mail Queue nicht deaktiviert wurde (siehe **Mail Processing** 147 Sektion **Ruleset Generator** **Advanced Options "**Run in queueless mode**"**) werden durch SEPPmail-Appliance verarbeitete E-Mails bei Bedarf - zum Beispiel wenn das Zielsystem temporär nicht erreichbar ist oder aufgrund eines Greylisting Filters die E-Mail beim ersten Sendeversuch ablehnt - in einer Warteschlange zwischengespeichert. Das SEPPmail-System wird in regelmässigen Abständen versuchen die E-Mails der Warteschlange auszuliefern. Kann eine E-Mail trotz mehrmaliger Auslieferungsversuche nicht zugestellt werden, so wird der Absender darüber benachrichtigt und die E-Mail verworfen.
Der Inhalt dieser Warteschlange ist über die Schaltfläche **Show queued mails...** einzusehen. Ein erneuter Auslieferungsversuch der zwischengespeicherten E-Mails kann über die Schaltfläche **Retry to deliver queued mails...** forciert werden.

**Sektion Log Archive**

In dieser Sektion wird das maillog verwaltet. Die SEPPmail-Appliance lagert dabei jeweils ab erreichen von 30 MB in Archiv-Dateien aus. Über die Schaltfläche **Download complete log** wird die aktuelle Log-Datei sowie alle vorhandenen Archiv-Dateien in einem Stream in eine Datei (maillog.txt) heruntergeladen.
Über die Schaltfläche **Download log archive** werden lediglich alle Archive heruntergeladen. Somit können Die Archive im Anschluss von der Appliance via **Delete log archive** gelöscht werden.
Die ist zum Beispiel dann erforderlich, wenn der Speicherplatz der Log-Partition knapp wird (siehe Home 116 Sektion **Disk statistics** **Logs**).
Ein automatisches Löschen des maillog kann ebenfalls eingestellt werden (siehe **System** 119 Sektion **Log Cleanup** **Automatically delete log archives older than ? days**).

**Sektion Filter**

Über das Eingabefeld kann ein regulärer Ausdruck (regular expression) eingegeben werden, nach welchem durch klicken der Schaltfläche **Apply...** im gesamten maillog (aktuelles sowie alle Archive) gesucht wird. Über die beiden Drop-Down Menüs kann die Suche auf einen bestimmten Zeitraum eingeschränkt werden.
Das Suchergebnis wird in der Sektion **Mail Log (last 500)** angezeigt.

**Sektion Mail Log (last 500)**

© 2015 SEPPmail AG

Zeigt die letzten 500 maillog Einträge an.

| Spalte | Beschreibung |
|---|---|
| **Nr.** | Laufende Nummer der Log-Einträge. Durch klicken auf die Nummer werden Details zum Log-Eintrag angezeigt. |
| **Source IP** | Quell-IP-Adresse von welcher die E-Mail eingeliefert wurde. |
| **Date** | Datum und Uhrzeit des Vorgangs. |
| **From** | Absender E-Mail-Adresse |
| **To** | Empfänger E-Mail-Adresse. Diese wird je Nach Status farbig angezeigt:<br>schwarz: E-Mail wurde noch nicht verarbeitet oder direkt ausgeliefert. Dieser Status erscheint zum Beispiel auch bei als SPAM identifizierten E-Mails (siehe **Mail Processing** 147 **Ruleset Generator** **Protection Pack** **(Antivirus / Antispam** Check incoming mails for spam and redirect spam to (leave empty to reject spam):)<br>grün: E-Mail wurde erfolgreich ausgeliefert<br>orange: E-Mail konnte nicht ausgeliefert werden und wurde in der Warteschlange bis zum nächsten Auslieferungsversuch abgelegt<br>rot: E-Mail konnte nicht ausgeliefert werden und wurde zurückgewiesen. Eine Benachrichtigungsmail über diesen Vorgang geht an den Absender. |
| **Message-ID** | Eindeutige Kennummer der E-Mail. Mittels dieser ID kann auch auf anderen Komponenten - zum Beispiel Groupware Server oder AntiSpam Komponente - die E-Mail nachverfolgt werden. |
| **Subject** | Betreff der E-Mail. Dieser wird nur angezeigt, wenn die Anzeige nicht ausgeblendet wurde (siehe **Mail Processing** 147 Sektion **Ruleset Generator** **General Settings** "Show message subject in logs"). |
| **Size** | Grösse der E-Mail. |

© 2015 SEPPmail AG

## 7.12 Statistics

In diesem Menü werden diverse Messgrössen grafisch dargestellt. Dabei wird für jede Sektion jeweils

- die letzten 24 Stunden (Today)
- die letzte Woche (Last Week)
- der letzte Monat (Last Month)
- das letzte Jahr (Last Year)
- die letzten drei Jahre (Last 3 Years)

dargestellt.

### Sektion Throughput Visualisation

Die Grafiken dieser Sektion stellen den E-Mail Durchsatz dar.

| Graph Farbe | Beschreibung |
|---|---|
| grün | Zeigt die Gesamtzahl der empfangenen E-Mails an. |
| blau | Zeigt die Gesamtzahl der gesendeten E-Mails an. |
| rot | Zeigt die Gesamtzahl der verschlüsselten E-Mails an. |
| lila | Zeigt die Gesamtzahl der entschlüsselten E-Mails an. |

### Sektion Technology Visualisation

Die Grafiken dieser Sektion stellen die Häufigkeit der verwendeten Verschlüsselungstechnologien dar.

| Graph Farbe | Beschreibung |
|---|---|
| blau | Zeigt die Gesamtzahl der mittels GINA Technologie verschlüsselten E-Mails an. |
| grün | Zeigt die Gesamtzahl der mittels S/MIME Technologie verschlüsselten E-Mails an. S/MIME signierte E.Mails werden nicht dargestellt. |
| rot | Zeigt die Gesamtzahl der mittels openPGP Technologie verschlüsselten E-Mails an. |
| lila | Zeigt die Gesamtzahl der mittels Domain Verschlüsselung verschlüsselten E-Mails an. |

### Sektion Spam Visualisation

Die Grafiken dieser Sektion stellen die Aktionen der SPAM Abwehrmassnahmen dar, sofern das Protection Pack (VSPP) lizensiert und aktiviert wurde.

© 2015 SEPPmail AG

| Graph Farbe | Beschreibung |
|---|---|
| rot | Zeigt die Gesamtzahl aller aufgrund des Greylistings abgewiesenen E-Mails an. |
| blau | Zeigt die Gesamtzahl der aufgrund der Realtime Blackhole List (RBL) Funktion abgewiesenen E-Mails an. |
| lila | Zeigt die Gesamtzahl der aufgrund der SPAM Erkennung abgewiesenen E-Mails an. |
| grün | Zeigt die Gesamtzahl der empfangenen E-Mails an. |

**Sektion CPU Usage Visualisation**

Die Grafiken dieser Sektion stellen die Prozessorauslastung der Appliance dar.

| Graph Farbe | Beschreibung |
|---|---|
| grün | Zeigt die vom System verursachte Prozessor Auslastung in Prozent an. |
| rot | Zeigt die benutzerbezogene Prozessor Auslastung in Prozent an. |
| blau | Zeigt die freien Prozessor Ressourcen in Prozent an. |

**Sektion Memory Usage Visualisation**

Die Grafiken dieser Sektion stellen die Speicherauslastung der Appliance in Megabyte (MB) dar.

| Graph Farbe | Beschreibung |
|---|---|
| grün | Zeigt den aktiv in Benutzung befindlichen Speicher an. |
| rot | Zeigt den belegten Speicher an. |
| hellblau | Zeigt den belegten Auslagerungsspeicher an. |
| dunkelblau | Zeigt die Grösse des zur Verfügung stehenden Auslagerungsspeichers an. |
| schwarz | Zeigt die freien Speicher Ressourcen an. |

© 2015 SEPPmail AG

## 7.13 Users

In diesem Menü werden die auf der SEPPmail-Appliance vorhandenen Benutzer angezeigt.
Die Anlage von Benutzern kann automatisch oder manuell (siehe Mail Processing 147 Ruleset Generator **UserCreation**) erfolgen.

| Spalte | Beschreibung |
|---|---|
| **User ID** | Zeigt die "User ID" des jeweiligen Benutzers an.<br>Diese entspricht bei automatisch generierten Benutzern immer der E-Mail Adresse. |
| **Name** | Zeigt den Namen des jeweiligen Benutzers an.<br>Diese entspricht bei automatisch generierten Benutzern dem Anzeigenamen des Absenders, sofern vorhanden. Andernfalls wird auch hier die E-Mail Adresse angezeigt. |
| **E-Mail** | Zeigt die E-Mail Adresse des Benutzers an. |
| **openPGP** | Zeigt die Anzahl der für den Benutzer vorhandenen openPGP Schlüssel an. |
| **S/MIME** | Zeigt die Anzahl der für den Benutzer vorhandenen S/MIME Schlüssel an. |
| **State** | Zeigt den Status des Benutzers an. Im Regelfall ist dieses Feld leer.<br>Bei technischen Benutzern kann der Status auf "inaktiv" gesetzt werden (siehe Untermenü Benutzerdetails 204 User Data **Encryption Settings**). Inaktive Benutzer sind nicht in der Lage zu verschlüsseln oder signieren und benötigen somit auch keine Benutzerlizenz. |

Durch Klicken auf die **User ID** wird das Untermenü Benutzerdetails 204 geöffnet.

Sollen Benutzer manuell eingerichtet werden, so erfolgt dies über die Schaltfläche **Create new user account...** (siehe Untermenü Create new user account 208).

Über die Schaltfläche **Password Policy** werden die Passwort Regeln für SEPPmail-Benutzer definiert (siehe Untermenü Password Policy 209).

Die Eingabefeld mit der Schaltfläche **Filter...** dient der Suche nach Benutzern.

© 2015 SEPPmail AG

### 7.13.1 Untermenü Benutzerdetails

**Sektion User Data**

| Parameter | Beschreibung | |
|---|---|---|
| **User ID** | Zeigt die "User ID" des jeweiligen Benutzers an.<br>Diese entspricht bei automatisch generierten Benutzern immer der E-Mail Adresse. | |
| Full Name | Zeigt den Namen des jeweiligen Benutzers an.<br>Diese entspricht bei automatisch generierten Benutzern dem Anzeigenamen des Absenders, sofern vorhanden. Andernfalls wird auch hier die E-Mail Adresse eingesetzt. | |
| **E-Mail** | Zeigt die E-Mail Adresse des Benutzers an. | |
| Password | Optional kann hier einem Benutzer ein Passwort vergeben werden.<br>Das Passwort muss den Passwort Regeln entsprechen (siehe Untermenü Password Policy 209).<br><br>**Hinweis:**<br>Die Vergabe eines Passwortes ist für das Nutzen der Appliance nicht notwendig. Durch die Vergabe eines Passwortes wird es einem Benutzer ermöglicht, sich interaktiv an der Appliance - also der Administrationsoberfläche - anzumelden. Hierfür muss der jeweilige Benutzer zusätzlich den entsprechenden Gruppen (siehe Groups 213) zugeordnet werden. | |
| **Encryption Settings** | May not encrypt mails | Untersagt dem Benutzer E-Mails zu verschlüsseln. Fordert der Benutzer trotzdem Verschlüsselung an, so würde die E-Mail abgewiesen (bounced) werden. |
| | May not sign mails | Untersagt dem Benutzer E-Mails zu signieren. Fordert der Benutzer trotzdem Verschlüsselung an, so würde die E-Mail abgewiesen (bounced) werden. |
| | Sind beide Optionen gewählt, so wird für den Benutzer keine Userlicense in Anspruch genommen. Dies bietet sich zum Beispiel bei technischen Benutzern an, welche keine E-Mails in das Internet versenden (zum Beispiel Backup-Benutzer). | |
| **Notification Settings** | always receives notification when recipient reads GINA mail | An dieser Stelle kann für jeden Benutzer individuell eingestellt werden, ob er GINA Lesebestätigungen erhalten soll. Ist diese Option bereits global in den GINA Domain Settings (siehe Edit GINA Settings 165 Extended Settings **Sender always receives notification when recipient reads GINA mails**) ausgewählt, so ist dieser Punkt ausgegraut. |
| **Usage Statistics** | Zeigt die Nutzungsstatistik des Benutzers an. | |
| | **Last outgoing mail** | Zeitpunkt der letzten ausgehenden E-Mail |
| | **S/MIME encrypted mails sent** | Anzahl der versendeten E-Mails, welche mittels S/MIME-Technologie verschlüsselt wurden |
| | **S/MIME encrypted mails received** | Anzahl der empfangenen E-Mails, welche mittels S/MIME-Technologie verschlüsselt waren |
| | **S/MIME signed** | Anzahl der versendeten E-Mails, welche mittels S/MIME- |

© 2015 SEPPmail AG

| Parameter | Beschreibung | |
|---|---|---|
| | **mails sent** | Technologie signiert wurden |
| | **S/MIME signed mails received** | Anzahl der empfangenen E-Mails, welche mittels S/MIME-Technologie signiert waren |
| | **openPGP encrypted mails sent** | Anzahl der versendeten E-Mails, welche mittels openPGP-Technologie verschlüsselt wurden |
| | **openPGP encrypted mails received** | Anzahl der empfangenen E-Mails, welche mittels -Technologie verschlüsselt waren |
| | **Webmail encrypted mails sent** | Anzahl der versendeten E-Mails, welche mittels GINA-Technologie verschlüsselt wurden |
| | **Webmail encrypted mails received** | Anzahl der mittels GINA-Technologie empfangenen E-Mails |
| | **S/MIME Domain encrypted mails sent** | Anzahl der versendeten E-Mails, welche mittels S/MIME-Technologie domänenverschlüsselt wurden |
| | **S/MIME Domain encrypted mails received** | Anzahl der empfangenen E-Mails, welche mittels S/MIME-Technologie domänenverschlüsselt waren |
| | **openPGP Domain encrypted mails sent** | Anzahl der versendeten E-Mails, welche mittels openPGP-Technologie domänenverschlüsselt wurden |
| | **openPGP Domain encrypted mails received** | Anzahl der empfangenen E-Mails, welche mittels openPGP-Technologie domänenverschlüsselt waren |

### Sektion Group Membership

In dieser Sektion werden die Gruppenzugehörigkeiten des Benutzers angezeigt (siehe auch Groups 213)

### Sektion S/MIME

| Serial | Certificate Authorothy | Issued on | Expires on |
|---|---|---|---|
| Zeigt die Seriennummern der Zertifikate an. | Zeigt die ausstellende CA an | Ausstelldatum des Keys TT-MM-JJJJ | Ablaufdatum des Keys TT-MM-JJJJ |

Durch Klicken des **Fingerprint**s wird ein Untermenü mit Details zum Key geöffnet. Dieses bietet die Möglichkeit den öffentlichen Schlüssel (Zertifikat) herunterzuladen beziehungsweise das Schlüsselpaar zu löschen.

© 2015 SEPPmail AG

Über die Schaltfläche **Import S/MIME Certificate...** kann ein bereits vorhandenes Zertifikat - zum Beispiel ein gekauftes einer Trusted CA - importiert werden (siehe **Mail System** Untermenü "Add/ Edit Managed Domain" Untermenü **Import S/MIME Key** 142).

Über die Schaltfläche **Generate S/MIME Certificate...** wird durch die integrierte CA ein neues Schlüsselpaar auf der Appliance generiert.
Ist eine MPKI eingerichtet (siehe **CA** 185 **External CA**), so erscheint entsprechend der verfügbaren CA die Schaltfläche **Generate <MPKI> Certificate...**. Durch klicken dieser Schaltfläche wird ein Schlüsselpaar generiert. Der öffentliche Schlüssel wird dabei durch die MPKI signiert und steht somit als trusted Zertifikat zur Verfügung.

### Sektion openPGP

In dieser Sektion werden die openPGP Domänen-Schlüssel angezeigt, sofern vorhanden.

| Key ID | User ID | Issued on | Expires on |
|---|---|---|---|
| Zeigt die Key IDs der vorhandenen openPGP-Keys an | Zeigt die zur Key ID zugehörige User ID an. Diese entspricht der E-Mail-Adresse des Benutzers. | Ausstelldatum des Keys TT-MM-JJJJ | Ablaufdatum des Keys TT-MM-JJJJ |

Über die Schaltfläche **Import openPGP key...** kann ein bereits vorhandenes Schlüsselpaar importiert werden (siehe **Mail System** Untermenü "Add/Edit Managed Domain" Untermenü **Import openPGP Key** 141).

Über die Schaltfläche **Generate new openPGP key** wird ein neues Schlüsselpaar auf der Appliance generiert. Die Laufzeit sowie das automatische Aktualisieren der so erzeugten Schlüssels entspricht der unter **CA** **internal CA Settings** Validity in days (siehe Menü **CA** 185) eingegebenen.

Durch Klicken der **Key ID** wird ein Untermenü mit Details zum Key geöffnet. Dieses bietet die Möglichkeit den öffentlichen Schlüssel herunterzuladen beziehungsweise das Schlüsselpaar zu löschen.

### Sektion Remote POP3

Wurde unter **Mail System** 129 **Managed Domains** die Option **Fetch Mail from remote POP3 server** gewählt, so können die POP3 beziehungsweise IMAP Zugangsdaten für den jeweiligen Benutzer an dieser Stelle eingegeben werden. Die SEPPmail-Appliance wird alle drei Minuten E-Mails abholen. Dabei wird POP3S beziehungsweise IMAPS präferiert.

| Parameter | Beschreibung |
|---|---|
| User ID | Eingabe der User ID zur Anmeldung am POP3/IMAP Konto. In der Regel entspricht die User ID der E-Mail Adresse. |
| Password | Zur User ID gehöriges Passwort. |
| Mail server | POP3 beziehungsweise IMAP Server von welchem E-Mails abgeholt werden sollen. |

© 2015 SEPPmail AG

**Sektion Customer**

Diese Sektion erscheint nur bei mandantenfähigen Systemen (siehe Menüpunkt **Customers** 223).
Sie ermöglicht die Zuordnung des Benutzers zu einem Mandanten.

**Hinweis:**
Die Zuordnung von Benutzern zu den jeweiligen Mandanten erfolgt normalerweise automatisch anhand der in der E-Mail Adresse enthaltenen E-Mail Domäne der E-Mail Adresse. Von Änderungen ist deshalb im Normalfall abzusehen.
Eine erneute automatische Zuordnung kann über die Auswahl "**Reset**" angestossen werden.

Alle vorgenommenen Änderungen werden über die Schaltfläche **Save changes** gespeichert.
Das Löschen eines Users erfolgt über **Delete User**.

**Hinweis:**
Ist einem Benutzer gültiges Schlüsselmaterial zugeordnet, so muss dieses vor dem Löschen des Benutzer gelöscht werden. Andernfalls erscheint zunächst eine entsprechende Warnmeldung.

© 2015 SEPPmail AG

### 7.13.2 Untermenü Create new user account

**Sektion User Data**

| Parameter | Beschreibung |
|---|---|
| User ID | Eingabe einer Eindeutigen "User ID" für den neuen Benutzer.<br>Es empfiehlt sich - wie bei automatisch generierten Benutzern - auch an dieser Stelle die E-Mail Adresse zu verwenden, da hierdurch die Eindeutigkeit gewährleistet wird.<br> <br>**Hinweis:**<br>Diese Eingabe kann in den Benutzerdetails 204 nicht mehr geändert werden. |
| Full Name | Zeigt den Namen des jeweiligen Benutzers an.<br>Diese entspricht bei automatisch generierten Benutzern immer der E-Mail Adresse. |
| E-Mail | Zeigt die E-Mail Adresse des Benutzers an.<br> <br>**Hinweis:**<br>Diese Eingabe kann in den Benutzerdetails 204 nicht mehr geändert werden. |
| Password | Optional kann hier einem Benutzer ein Passwort vergeben werden.<br>Das Passwort muss den Passwort Regeln entsprechen (siehe Untermenü Password Policy 209).<br> <br>**Hinweis:**<br>Die Vergabe eines Passwortes ist für das Nutzen der Appliance nicht notwendig. Durch die Vergabe eines Passwortes wird es einem Benutzer ermöglicht, sich interaktiv an der Appliance - also der Administrationsoberfläche - anzumelden. Hierfür muss der jeweilige Benutzer zusätzlich den entsprechenden Gruppen (siehe Groups 213) zugeordnet werden. |

Über die Schaltfläche **Create account** wird der Benutzer angelegt und kann im Anschluss weiter bearbeitet werden (siehe Untermenü Benutzerdetails 204).
**Cancel** bricht den Vorgang ab.

© 2015 SEPPmail AG

### 7.13.3 Untermenü Password Policy

**Sektion Password Settings for system (not GINA) accounts**

Die Vergabe eines Passwortes ist ausschliesslich für die Anmeldung an der Administrationsoberfläche notwendig. Die Berechtigungen für Benutzer mit Passwort wird über die Gruppenzugehörigkeit geregelt (siehe Groups 213).
Das heisst die hier definierten Passwort Regeln sind für die interaktive Anmeldung an der Administrationsoberfläche gültig.

| Parameter | Beschreibung |
|---|---|
| **Minimum password length: ?** | Auswahl der minimalen Passwort Länge (4 bis 16 Zeichen). |
| **Must contain at least one lower case letter** | Definiert, ob ein Kleinbuchstabe im Passwort enthalten sein muss. |
| **Must contain at least one upper case letter** | Definiert, ob ein Grossbuchstabe im Passwort enthalten sein muss. |
| **Must contain at least one number** | Definiert, ob eine Ziffer im Passwort enthalten sein muss. |
| **Must contain at least one special character** | Definiert, ob ein Sonderzeichen im Passwort enthalten sein muss. |
| **Must not contain own name, user name or e-mail address** | Definiert, ob das Passwort den eigenen Namen oder E-Mail Adresse enthalten darf. |
| **Must be different from previous ? password(s)** | Definiert, mit wie vielen vorangegangenen Passwörter bei einem Passwortwechsel keine Übereinstimmung bestehen darf (1 bis 28). |
| **Must be changed at least every ? days** | Definiert, ob und nach wie vielen Tagen das Passwort geändert werden muss. |
| **Accounts are locked for ? minutes after ? failed login attempts.** | Definiert, nach wie vielen fehlgeschlagenen Fehlversuchen bei der Anmeldung (falsche Passworteingabe) für wie lange (in Minuten) der Zugang gesperrt wird. |

Über die Schaltfläche **Save** werden die angezeigten Einstellungen gesichert.
Mittels **Back** wird das Menü ohne Sicherung verlassen.

© 2015 SEPPmail AG

## 7.14 GINA Accounts

In diesem Menü werden die auf der SEPPmail-Appliance vorhandenen GINA-Benutzer angezeigt. Handelt es sich um ein mandantenfähiges System, so sind die Benutzer entsprechend der Mandanten aufgeteilt.

| Spalte | Beschreibung |
|---|---|
| **E-mail** | Die E-Mail Adresse gewährleistet bei SEPPmail-Benutzern die Eindeutigkeit. |
| **Account status** | Zeigt den Status des jeweiligen Benutzers an. Mögliche Status sind:<br>• **enabled**<br>Soll-Zustand<br>• **enabled (unregistered user)**<br>Benutzer welcher nach Erhalt der initialen GINA-E-Mail den Registrierungsprozess noch nicht abgeschlossen hat.<br>• **locked temporarely**<br>Gesperrter Benutzer. Nahere Details hierzu zeigt der **Last message status**.<br>• **locked temporarely (unregistered user)**<br>Benutzer welcher nach Erhalt der initialen GINA-E-Mail noch vor dem erfolgreichen Abschliessen des Registrierungsprozesses gesperrt wurde. Nahere Details hierzu zeigt der **Last message status**. |
| **Last message status** | Zeigt Informationen zur letzten Aktion des Benutzers an. Mögliche Status sind:<br>• **Last succesful login MMM TT, JJJJ hh:mm:ss**<br>Gibt Datum und Uhrzeit der letzten erfolgreichen Anmeldung an.<br>• **X unsuccessful login attempts**<br>Gibt die Anzahl der fehlgeschlagenen Anmeldeversuche an. |

Durch Klicken auf die **E-mail**-Adresse wird ein Untermenü mit Details zum jeweiligen GINA-Benutzer geöffnet (siehe Untermenü GINA-Benutzer-Details 211).

Sollen Benutzer manuell eingerichtet werden, so erfolgt dies über die Schaltfläche **Create new user account...** (siehe Untermenü Create new user account 208).

Die Eingabefeld mit der Schaltfläche **Filter...** dient der Suche nach GINA-Benutzern.

© 2015 SEPPmail AG

### 7.14.1 Untermenü Benutzer-Details

**Sektion User Data**

In diesem Untermenü werden Detailinformationen zum GINA-Benutzer angezeigt. Weiterhin dient diese Menü manuellen Passwort Rücksetzungen, zum Beispiel durch den Support (siehe Edit GINA Settings 165 **Sektion** Admin).

| Parameter | Beschreibung | |
|---|---|---|
| **Creation Info** | Zeigt<br>• wer gegebenenfalls die initiale GINA-E-Mail gesendet und somit den Benutzer generiert hat (Anzeige der E-Mail-Adresse bei unregistrierten, beziehungsweise "Created by..." bei bereits registrierten Benutzern)<br>• ob es sich um einen selbstregistrierten Benutzer handelt (Account...) | |
| **Name** | Hat sich der Benutzer registriert, so wird hier der von ihm bei der Registrierung eingetragene Name angezeigt. | |
| **E-Mail** | Zeigt die E-Mail Adresse des Benutzers an. | |
| **Password reminder** | Zeigt die vom Benutzer beim Registrieren angegebene Sicherheitsfrage für das Zurücksetzen des Passwortes an (wichtig für die Option "Hotline" in der Einstellung Edit GINA Settings 165 **Sektion** Security beziehungsweise Password Security Level) | |
| **Answer** | Vom Benutzer während des Registrierens eingetragene Antwort zur Sicherheitsabfrage | |
| Password | Eingabefelder für das manuelle Rücksetzen des Passwortes durch einen Administrator | |
| **Must Change Password** | ☐ | Legt fest, ob der Benutzer nach einem manuellen Rücksetzen des Passwortes dieses beim nächsten Anmelden ändern muss. |
| **Zip Attachement** | ☐ | Legt individuell für den Benutzer fest, ob dieser den Anhang des GINA-E-Mails statt im HTML- im ZIP-Format erhält. |
| **Account status** | ○ **locked** | Zeigt an ob der Benutzer gesperrt ist (zum Beispiel nach mehrfacher falscheingabe des Passwortes) beziehungsweise kann der Administrator den Benutzer durch Aktivieren des Buttons sperren. |
| | ○ **enabled** | Zeigt an ob der Benutzer aktiv ist beziehungsweise kann der Administrator den Benutzer durch Aktivieren des Buttons wieder in den Staus "Aktiv". |
| **External Authentication** | ☐ **Exclude this account from external authentication**<br>Ist die externe LDAP Authentisierung aktiviert (siehe auch Add/Edit Managed Domain 136 External Authentication) so kann diese durch Anhaken dieser Option für einzelne Accounts ausgehebelt werden.<br>Diese Option ist nur bei intern - das heisst der Managed Domain welcher auch das entsprechende GINA-Interface zugeordnet ist - zugeordneten Benutzern zu sehen. | |

© 2015 SEPPmail AG

| Parameter | Beschreibung |
|---|---|
| Password Security Level | Benutzer individuelle Einstellung für das Rücksetzverfahren des Passwortes. Diese Einstellung überschreibt die globale Einstellung unter **Edit GINA Settings** 165 **Sektion Security**. |
| Mobile number | Mobilfunknummer für das Zurücksetzen des Passwortes via SMS. |

**Sektion User Logs**

Durch klicken der Schaltfläche **Show user logs** wird ein detailliertes Log bezüglich der aktivitäten des jeweiligen GINA-Benutzers angezeigt.

Alle vorgenommenen Änderungen werden über die Schaltfläche **Save changes** gespeichert.
Das Löschen eines GINA-Benutzers erfolgt über **Delete Account**.

**Hinweis:**
Durch das Löschen eines GINA-Benutzers wird auch dessen Schlüssel unwiderruflich gelöscht. Somit kann er eventuell noch in seinem Postfach befindliche GINA-E-Mails nicht mehr lesen. Der Inhalt dieser E-Mails ist somit verloren!

© 2015 SEPPmail AG

## 7.15 Groups

In diesem Menü sind bereits administrative Benutzergruppen vorgegeben (siehe Tabelle). Diese dienen der Wirkungsmöglichkeiten einzelner Benutzer bei interaktiver Anmeldung an der Administrationsoberfläche (siehe auch Benutzerdetails 204 User Data Password)
Weiterhin besteht über die Schaltfläche **Create new user group...** weitere Gruppen zur Verwendung im Ruleset (siehe Mail Processing 147 Ruleset Generator **Custom Commands**) zu erzeugen.
Über die Schaltfläche **Edit...** kann die jeweilige Gruppe editiert (Gruppen Name und Beschreibung) sowie Benutzer zugeordnet werden.

| Gruppe | Beschreibung |
|---|---|
| **admin (Administrator)** | Alle Mitglieder dieser Gruppe sind dem Standardbenutzer **admin** gleichgestellt und haben uneingeschränkten administrativen Zugang zur Konfigurationsoberfläche mit allen Berechtigungen. Weiterhin erhalten Mitglieder dieser Gruppe die gleichen Informationen wie der "**statisticsadmin**" zugesandt.<br> **Hinweis:** Sollten administrative Aufgaben anfallen, so werden die Mitglieder dieser Gruppe darüber informiert. Somit sollte der Administrator der SEPPmail-Appliance unbedingt Mitglied dieser Gruppe sein. |
| **administrationadmin (GUI Access to Administration Section)** | Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Administration** in der Konfigurationsoberfläche. |
| **backup (Backup Operator )** | Dieser Gruppe ist eine Sonderbedeutung zugeordnet. Sie unterscheidet sich von den Systemgruppen für den Zugriff auf die Konfigurationsoberfläche dadurch, dass kein Zugriff auf die Konfigurationsoberfläche erfolgt. Alle Mitglieder dieser Gruppe erhalten das Systembackup des jeweiligen Systems einmal täglich via E-Mail. Das Systembackup wird täglich um 0.00 Uhr erzeugt und via E-Mail an alle Mitglieder dieser Gruppe gesendet. |
| **caadmin (GUI Access to CA Section)** | Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **CA** in der Konfigurationsoberfläche. |
| **clusteradmin (GUI Access to Cluster Section)** | Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Cluster** in der Konfigurationsoberfläche. |
| **domainkeysadmin (GUI Access to Domain Keys Section)** | Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Domain keys** in der Konfigurationsoberfläche. |
| **groupsadmin (GUI Access to Groups Section)** | Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Groups** in der Konfigurationsoberfläche. |
| **homeadmin (GUI Access to Home Section)** | Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Home** in der Konfigurationsoberfläche. |

© 2015 SEPPmail AG

| Gruppe | Beschreibung |
|---|---|
| **logsadmin (GUI Access to Logs Section)** | Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Logs** in der Konfigurationsoberfläche. |
| **mailprocessingadmin (GUI Access to Mail Processing Section)** | Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Mail Processing** in der Konfigurationsoberfläche. |
| **mailsystemadmin (GUI Access to Mail System Section)** | Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Mail System** in der Konfigurationsoberfläche. |
| **multiplecustomersadmin (Admin access to Customer settings in multitenant deployments)** | Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Customers** in der Konfigurationsoberfläche. |
| **openpgpkeysadmin (GUI Access to openPGP Keys Section)** | Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **openPGP public keys** in der Konfigurationsoberfläche. |
| **readonlyadmin (Read-only GUI Access to all sections)** | Alle Mitglieder dieser Gruppe haben ausschliesslich lesenden Zugriff auf alle Menüs der Konfigurationsoberfläche. |
| **ssladmin (GUI Access to SSL Section)** | Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **SSL** in der Konfigurationsoberfläche. |
| **statisticsadmin (GUI Access to Statistics Section)** | Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Statistics** in der Konfigurationsoberfläche. Zusätzlich erhalten alle Mitglieder dieser Gruppe einen täglichen System-Report des jeweiligen Systems. Der System-Report wird täglich um 0.00 Uhr erzeugt und via E-Mail an alle Mitglieder dieser Gruppe gesendet. |
| **systemadmin (GUI Access to System Section)** | Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **System** in der Konfigurationsoberfläche. |
| **usersadmin (GUI Access to Users Section)** | Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Users** in der Konfigurationsoberfläche. |
| **webmailaccountsadmin (GUI Access to Webmail Accounts Section)** | Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **Webmail accounts** in der Konfigurationsoberfläche. |
| **x509certificatesadmin (GUI Access to X.509 Certificates Section)** | Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **X.509 Certificates** in der Konfigurationsoberfläche. |
| **x509rootcertificatesadmin (GUI Access to X.509 Root Certificates Section)** | Alle Mitglieder dieser Gruppe haben Zugriff auf das Menü **X.509 Root Certificates** in der Konfigurationsoberfläche. |

© 2015 SEPPmail AG

## 7.16 LFM accounts

In diesem Menü werden die auf der SEPPmail-Appliance vorhandenen LFM-Benutzer angezeigt. Handelt es sich um ein mandantenfähiges System, so sind die Benutzer entsprechend der Mandanten aufgeteilt.

| Spalte | Beschreibung |
|---|---|
| **E-mail** | E-Mail Adresse desLFM-Benutzers. |
| **Account status** | Zeigt den Status des jeweiligen Benutzers an. Mögliche Status sind:<br>• **inactive**<br>Interne Benutzer welche mehr als vier Wochen keine LFM-Mail versendet haben werden in den Status "inactive" versetzt. Hierdurch wird die bis dahin belegte LFM-Lizenz wieder frei.<br>• **active**<br>Interne Benutzer mit aktiver LFM-Lizenz. |
| **Account last used** | Zeigt an, wann der LFM Benutzer zuletzt eine grosse Datei versendet hat. Bei aktiven Benutzern lässt sich daraus schliessen, wann dieser auf inaktiv gesetzt wird und somit die Lizenz frei gibt, sofern in der Zwischenzeit nicht eine weitere grosse Datei durch ihn versendet wird. |

© 2015 SEPPmail AG

## 7.17 OpenPGP public keys

**Sektion Local openPGP Keys**

In dieser Sektion werden die der Appliance bekannten öffentlichen openPGP Schlüssel von Kommunikationspartnern angezeigt.

| Key ID | E-mail addresses | User Name | Issued on | Expires on |
|---|---|---|---|---|
| Zeigt die Key IDs der vorhandenen openPGP-Keys an | Zeigt die dem Schlüssel zueordnete/n E-Mail Adresse/n | Zeigt die zur Key ID zugehörige User ID an. Diese entspricht der E-Mail-Adresse des Benutzers. | Ausstelldatum des Keys TT-MM-JJJJ | Ablaufdatum des Keys TT-MM-JJJJ |

Durch Klicken der **Key ID** wird ein Untermenü mit Details zum Key geöffnet. Dieses bietet die Möglichkeit den öffentlichen Schlüssel herunterzuladen beziehungsweise das Schlüsselpaar zu löschen.

Das Eingabefeld mit der Schaltfläche **Filter...** dient der Suche nach nach entsprechenden Schlüsseln anhand einer der in der Tabelle aufgeführten Merkmale.

Über die Schaltfläche **Import openPGP key...** kann ein vorhandener Schlüssel eines Kommunikationspartners - nach Prüfung (Hash) - importiert werden. Im Anschluss steht dieser Schlüssel für das Verschlüsseln bereit.

© 2015 SEPPmail AG

## 7.18 X.509 Certificates

In diesem Menü werden die für die S/MIME Verschlüsselung zur Verfügung stehenden Zertifikate wie folgt angezeigt.

| Spalte | Beschreibung |
|---|---|
| **E-mail Address** | Zeigt E-Mail Adresse (RFC822 Name) des Schlüsselinhabers an. |
| **Certificate Subject** | Zeigt das X.509 Subject an. |
| **Serial Number** | Seriennummer des Zertifikats. |
| **Fingerprint** | Zeigt den Fingerprint (Hash) des Zertifikates an. |
| **Issued on** | Ausstelldatum des Zertifikats in der Form TT-MM-JJJJ |
| **Expires on** | Ablaufdatum des Zertifikats in der Form TT-MM-JJJJ |

Durch Klicken auf die E-Mail Adresse werden Details zum Zertifikat angezeigt. Dieses bietet die Möglichkeit den öffentlichen Schlüssel (Zertifikat) herunterzuladen beziehungsweise das Schlüsselpaar zu löschen.

Das Eingabefeld mit der Schaltfläche **Filter...** dient der Suche nach nach entsprechenden Zertifikaten anhand einer der in der Tabelle aufgeführten Merkmale.

Über die Schaltfläche **Import S/MIME Certificate...** kann ein vorhandenes Zertifikat eines Kommunikationspartners importiert werden. Im Anschluss steht dieses Zertifikat für das Verschlüsseln bereit - auch wenn die Zertifikatskette nicht geprüft werden kann (siehe auch **X.509 Root Certificates** 218). In der Regel werden die Zertifikate von Kommunikationspartnern aus deren E-Mail Signaturen automatisch eingesammelt. Dies funktioniert allerdings nur dann, wenn der Aussteller des Zertifikates bei den **X.509 Root Certificates** 218 eingetragen ist und eine entsprechende Vertrauensstellung (Trusted) vorhanden ist. Das heisst die Zertifikatskette muss für die SEPPmail-Appliance nachvollziehbar sein.

Die Schaltfläche **Clean up duplicate certificates...** entfernt eventuell doppelt vorhandenen Zertifikate.
Über die Schaltfläche **Delete expired certificates...** werden alle Zertifikate von dr Appliance entfernt, bei welchen das "**Expires on**" Datum überschritten ist. Damit wird bei Bedarf auch gewährleistet, dass diese Zertifikate nicht mehr für die Verschlüsselung verwendet werden. Im Standard verwendet die Appliance auch abgelaufene Zertifikate, natürlich nur wenn kein aktuelles zur Verfügung steht.

© 2015 SEPPmail AG

## 7.19 X.509 Root Certificates

In diesem Menü wird die Vertrauensstellung zu den einzelnen Zertifizierungsstellen (CA) verwaltet. Root Zertifikate welche nicht bekannt sind werden aus signierten E-Mails eingesammelt und mit dem Status "?" (unbekannt) gespeichert. Eine Einstufung dieser Zertifizierungsstellen muss durch den Administrator vorgenommen werden. Somit wächst das System dynamisch.
Angezeigt werden die Root Zertifikate wie folgt.

| Spalte | Beschreibung |
|---|---|
| **Trust State** | Zeigt die Vertrauensstellung an. Mögliche Status sind "trusted" (vertrauenswürdig), "untrusted" (nicht vertrauenswürdig) und "?" (unbekannt). Bei unbekanntem Status ist ein Eingreifen des Adminstrators erforderlich. Dieser muss entscheiden, ob der CA vertraut werden soll oder nicht. Sind Zertifikate mit dem Status "?" vorhanden, so werden diese dem Administrator (siehe Menü **Groups** 213) im täglichen Report gemeldet.<br>Durch Klicken auf den Vertrauensstatus des Zertifikates können Details eingesehen und die Vertrauensstellung angepasst werden (siehe Untermenü **Vertrauensstellung** 219) |
| **Issued to** | Zeigt an, für wen das Zertifikat ausgestellt wurde. |
| **Issued by** | Zeigt an, von wem das Zertifikat ausgestellt wurde. |
| **Issued on** | Ausstelldatum des Zertifikats in der Form TT-MM-JJJJ |
| **Expires on** | Ablaufdatum des Zertifikats in der Form TT-MM-JJJJ |
| **Fingerprint** | Zeigt den Fingerprint (Hash) des Zertifikates an. |

Das Eingabefeld mit der Schaltfläche **Filter...** dient der Suche nach nach entsprechenden Zertifikaten anhand einer der in der Tabelle aufgeführten Merkmale.

Über die Schaltfläche **Import S/MIME Root Certificate...** kann ein vorhandenes Zertifikat einer Zertifizierungsstelle importiert werden. Hier können zum Beispiel auch Root Zertifikate einer Self-Signed-CA eines vertrauenswürdigen Kommunikationspartners eingetragen werden. Somit werden auch dessen Self-Signed Zertifikate als vertrauenswürdig eingestuft.

© 2015 SEPPmail AG

### 7.19.1 Untermenü Vertrauensstellung

**Sektion Issued To**

Diese Sektion zeigt Informationen über den Inhaber des CA-Zertifikates.
Abhängig vom Zertifikat müssen nicht alle hier aufgeführten Parameter vorhanden sein.

| Parameter | Beschreibung |
|---|---|
| **Name (CN)** | Gibt den Namen der eigenen CA an |
| **E-Mail Address** | In der Regel der wird die E-Mail-Adresse des Verwalters der eigenen CA oder dessen Abteilung eingetragen. |
| **Org. Unit (OU)** | Organisationseinheit wie zum Beispiel ein Abteilungsname wie "Sicherheit" |
| **Organization (O)** | Gibt die Organisation an, für welche das Zertifikat ausgestellt wurde, zum Beispiel "Firma" |
| **Locality (L)** | Standort zum Beispiel eine Stadt wie "Neuenhof" |
| **State (ST)** | Bundesland, Kanton, Provinz oder Ähnliches, zum Beispiel "AR" für "Appenzell Ausserrhoden" |
| **Country (C)** | Land, zum Beispiel "CH" für "Schweiz" |
| **Serial No.** | Seriennummer des Zertifikats |

**Sektion Issued By**

Diese Sektion zeigt Informationen über den Aussteller des CA-Zertifikates (Root-Zertifikat).
Abhängig vom Aussteller müssen nicht alle hier aufgeführten Parameter vorhanden sein.

| Parameter | Beschreibung |
|---|---|
| **Name (CN)** | Name der ausstellenden CA |
| **E-Mail Address** | In der Regel eine E-Mail-Adresse für Supportanfragen an den Aussteller |
| **Org. Unit (OU)** | Gibt eine Organisationseinheit des Ausstellers an |
| **Organization (O)** | Gibt die ausstellende Organisation an |
| **Locality (L)** | Gibt den Standort des Ausstellers an |
| **State (ST)** | Gibt ein Bundesland, Kanton, Provinz oder Ähnliches des Ausstellers an |
| **Country (C)** | Gibt das Land des Ausstellers an |

© 2015 SEPPmail AG

### Sektion Validity

Gibt die Gültigkeit des eigenen CA-Zertifikates an.

| Parameter | Beschreibung |
|---|---|
| **Issued on** | Ausstelldatum des Zertifikates |
| **Expires on** | Ablaufdatum des Zertifikates |

### Sektion Fingerprint

Gibt den Hash des eigenen CA-Zertifikates an.

| Parameter | Beschreibung |
|---|---|
| **Hashalgorhytmus des Zertifikates, zum Beispiel SHA1** | Der Fingerprint dient zur Überprüfung eines Zertifikats. Beispiel eines SHA1 Fingerprints:<br>48:2D:99:B1:64:C1:14:9C:B3:F2:C0:8D:FA:7F:40:9F:22:F5:11:F5 |

### Sektion Comment

An dieser Stelle kann ein persönlicher Kommentar zum Zertifikat eingegeben werden, zum Beispiel weshalb die entsprechende Vertrauensstellung gewählt wurde.
Mit **Save Comment** wird dieser Kommentar gespeichert.

Über die Schaltfläche **Download Certificate** besteht die Möglichkeit das Zertifikat im CRT-Format zu speichern.
Je nach Vertrauensstellung wird die Schaltfläche **Trust this certificate**, über welche dem Zertifikat das Vertrauen bestätigt wird oder **Untrust this Certificate**, durch welche das Vertrauen abgelehnt wird, vorhanden.
Über **Delete Certificate** wird das Zertifikat von der SEPPmail-Appliance gelöscht. Wird im Anschluss eine E-Mail empfangen, welche mit einem Schlüssel dieser Zertifizierungsstelle signiert wurde, so wird das Zertifikat wieder mit dem Truststatus "?" in der Appliance gespeichert.

© 2015 SEPPmail AG

## 7.20 Domain Certificates

Domänen Zertifikate werden für die Domänenverschlüsselung, also die E-Mail Verschlüsselung zwischen zwei Appliances benötigt. Da die Zertifikate in der Regel direkt durch die Administratoren ausgetauscht werden, reichen an dieser Stelle im Normalfall Self-Signed Zertifikate aus. Aufgeführt sind hier die öffentlichen Schlüssel der Kommunikationspartner, zu denen Domänenverschlüsselt werden soll. Die Schlüssel zu den intern in der SEPPmail-Appliance verwalteten E-Mail Domänen sind unter **Add/Edit Managed Domain** 136 je nach Verschlüsselungstechnologie in der Sektion **openPGP Domain Encryption** oder **S/MIME Domain Encryption** zu finden. Die öffentlichen Schlüssel für diese Domänen können je nach GINA-Konfiguration vom Kommunikationspartner auch über das GINA-Web-Portal auf sicherem Wege heruntergeladen werden (siehe **Edit GINA Settings** 165 **Extended Settings** **Enable S/MIME certificate / openPGP key search and management in GINA**).

### Sektion openPGP Domain Keys

Zeigt die Schlüssel aller E-Mail Domänen an, zu denen hin mittels openPGP verschlüsselt wird. Diesen Domänen sollte im Gegenzug der öffentliche openPGP Key der durch diese SEPPmail-Appliance verwalteten E-Mail Domäne(n) bekannt sein.

| Mail Domain | Key ID | Issued on | Expires on |
|---|---|---|---|
| Gibt die E-Mail Domäne an, für welche der Schlüssel gültig ist. Durch klicken auf die Domäne werden Details zum Schlüssel angezeigt. Ebenso wird die hierdurch die Möglichkeit geboten, den Key im ASC-Format zu speichern oder zu löschen. | Zeigt die Key IDs der vorhandenen openPGP-Keys an | Ausstelldatum des Keys TT-MM-JJJJ | Ablaufdatum des Keys TT-MM-JJJJ |

Über die Schaltfläche Import **Import openPGP Key...** besteht die Möglichkeit Schlüssel weiterer Kommunikationspartner (E-Mail Domänen) aufzunehmen.

### Sektion SMIME Domain Certificates

Zeigt die Zertifikate aller E-Mail Domänen an, zu denen hin mittels S/MIME verschlüsselt wird. Diesen Domänen sollte im Gegenzug das S/MIME Zertifikatder durch diese SEPPmail-Appliance verwalteten E-Mail Domäne(n) bekannt sein.

| Spalte | Beschreibung |
|---|---|
| **Mail Domain** | Zeigt E-Mail Adresse (RFC822 Name) des Schlüsselinhabers an. |
| **E-mail Address** | (Pseudo-)E-Mail Adresse für die Domänenverschlüsselung |
| **Serial Number** | Seriennummer des Zertifikats. |
| **Issued on** | Ausstelldatum des Zertifikats in der Form TT-MM-JJJJ |

© 2015 SEPPmail AG

| Spalte | Beschreibung |
|---|---|
| **Expires on** | Ablaufdatum des Zertifikats in der Form TT-MM-JJJJ |

Über die Schaltfläche Import **Import S/MIME Certificate...** besteht die Möglichkeit Zertifikate weiterer Kommunikationspartner (E-Mail Domänen) aufzunehmen.

### Sektion Managed Domain Certificates

Da SEPPmail-Appliances im Standard (siehe Mail System 129 Managed Domains "**Automatically create and publish S/MIME domain keys for all domains**") am sogenannten "Managed Domain Service" teilnehmen, findet zwischen SEPPmail-Appliances immer eine Domänenverschlüsselung statt, ohne explizit Schlüsselmaterial austauschen zu müssen. Dies geschieht automatisch über den SEPPmail-Key Server.
Das automatische Herunterladen der öffentlichen Schlüssel anderer Appliances erfolgt dabei über die Option "**Auto-Update SMIME Domain Certificates**". Im Bedarfsfall (zum Beispiel bei Hinzukommen eines neuen, bekannten Kommunikationspartners) kann ein sofortiges Herunterladen neu hinzugekommenr Schlüssel über die Schaltfläche **Update Domain Certificates...** forciert werden.
Die Anzahl der über diesen Dienst verfügenden E-Mail Domänen wird im Text darunter angegeben.
Um festzustellen, ob ein Kommunikationspartner ebenfalls am SEPPmail-Managed-Domain-Service teilnimmt, bietet das Eingabefeld mit der Schaltfläche **Search Domain Certificate...** eine entsprechende  Möglichkeit nach dem E-Mail Domänennamen zu suchen.
Die Domänen, zu welchen in den letzten drei Monaten über den Managed Domain Service verschlüsselt kommuniziert wurde werden in der Tabelle dieser Sektion aufgeführt.

**Hinweis:**
Die Domänenverschlüsselung ist bei der SEPPmail-Appliance bereits in der Basis-Lizenz enthalten. Das heisst diese wird auch für Absender verwendet, welche über kein Benutzerkonto (siehe Users 203) verfügen, ohne Mehrkosten zu produzieren.

© 2015 SEPPmail AG

## 7.21 Customers

Ist eine Multitenancy Lizenz vorhanden, so lässt sich in diesem Menü die Mandantenfähigkeit des Systems aktivieren, beziehungsweise die Mandanten verwalten.

### Sektion Multiple Customers

Über die Schaltfläche **Enable** lässt sich die Mandantenfähigkeit aktivieren. Sollte diese bereits aktiv sein, so bietet sich die Möglichkeit über das DropDown-Menü einen Mandanten auszuwählen und über die Schaltfläche **Delete...** zu löschen oder über **Edit...** zu bearbeiten. Weiter bietet die Schaltfläche **Create new customer...** die Möglichkeit einen neuen Mandanten anzulegen.
Dabei existieren nach Anschalten der Mandantenfähigkeit bereits zwei Standard Customers ("No Customer" und "Default Customer"), welche für die interne Verwaltung benötigt werden und keinesfalls gelöscht werden dürfen.

Wird bei einer bereits bestehenden Installation mit bereits vorhandenen GINA-Accounts nachträglich die Mandantenfähigkeit aktiviert, so werden diese Accounts zunächst dem "Default Customer" zugeordnet. Um das nachträgliche zuordnen der Accounts zum richtigen Mandanten zu erleichtern, wird angezeigt, aus welcher Managed Domain der Account erzeugt wurde.

Der "No Customer" bietet die Möglichkeit, einzelne Accounts - gegebenenfalls temporär - komplett aus der Mandantenfähigkeit auszuschliessen.
Ist bei einem nachträglichen Anschalten der Mandantenfähigkeit das sofortige zuordnen zu einem Mandanten aus dem "Default Customer" heraus nicht erwünscht - wenn der Account zum Beispiel einem später noch einzuirichtenden Mandanten zugeordnet werden soll - so kann dieser im "No Customer" quasi "zwischengeparkt" werden.

### Sektion Notes

Für einen Mandanten **muss** immer ein eigenes GINA-Interface angelegt werden (siehe gegebenenfalls **Create new GINA Domain** 164). Sollte der Mandant mehrere "Managed Domains" inne haben, so kann all diesen das gleiche GINA-Interface zugeordnet (siehe **Mail System** 129 **Managed Domains** **GINA Settings**) werden.

**Achtung:**
Keinesfalls darf ein GINA-Interface für mehrere Mandanten verwendet werden!

Externe Empfänger welche mit mehreren Mandanten mittels GINA kommunizieren, erhalten für jeden Mandanten ein eigenes GINA-Konto, mit den daraus resultierenden Einschränkungen (siehe **Edit GINA Settings** 165 **Extended settings**).

Öffentliche Schlüssel (siehe **openPGP public keys** 216 und **X.509 Certificates** 217) stehen grundsätzlich allen Mandanten für die Verschlüsselung zur Verfügung.

© 2015 SEPPmail AG

### 7.21.1 Untermenü Create new / Edit Settings for customer

Dieses Menü dient der Anlage neuer beziehungsweise der Verwaltung bereits vorhandener Mandanten auf dem SEPPmail-System.
Die Anlage neuer Mandanten kann manuell, oder durch den Import eines bereits bestehenden Mandanten Backup (zum Beispiel für den Umzug eines Mandanten auf eine andere Maschine) erfolgen.

#### Sektion Customer details

Diese Sektion enthält Informationen zum Mandanten und verhält sich je nach Modus - "Create" oder "Edit" - unterschiedlich.

| Parameter | Beschreibung |
|---|---|
| Customer | Eingabe des System-Namens für einen neuen Mandanten. Die Eingabe ist nur bei der Neuanlage möglich. Im Editier-Modus wird der Name lediglich angezeigt. |
| Customer Name | Anzeige-Name des Mandanten. |
| Customer Admin E-mail | E-Mail Adresse des Mandanten-Admin, welcher die Mandanten spezifischen Systemmeldungen erhalten soll. Dieser User erhält täglich automatisiert auch das Customer Backup. |
| Comment | Optionaler, frei wählbarer Kommentar. |
| **Creation info** | Systeminformationen zur Erzeugung des Mandanten. Dieses Feld ist erst nach dem Erzeugen des Mandanten, also im Editier-Modus zu sehen. |

Im "Create"-Modus wird der Benutzer mittels Schaltfläche **Create** mit den angegebenen Daten angelegt. Das System wechselt sodann in den Editier-Modus.
Im Editier-Modus werden vorgenommene Änderungen über die Schaltfläche **Change** übernommen.

#### Sektion Import Backup

Diese Sektion erscheint nur im "Create"-Modus und dient der Anlage neuer Mandanten durch den Import eines bereits bestehenden Mandanten Backups (zum Beispiel für den Umzug eines Mandanten auf eine andere Maschine) erfolgen.
Die vorhandene Backup Datei wird über die Schaltfläche **Import Backup File ...** eingespielt.

Alle folgenden Menüs sind nur im Editier-Modus zu sehen.

#### Sektion Customer administrators

Dient der Verwaltung von Mandanten-Admins. Mandanten Admins sind in der Lage sich interaktiv am System anzumelden und sehen die für sie relevanten Menüs **Login** 115, **Mail Processing** 147, **Logs** 199, und optional bei aktivierter Option **LFM accounts** 215. Dabei beschränkt sich die Anzeige in den Menüs ausschliesslich auf die Daten des jeweiligen Mandanten.
Bereits zugeordnete Mandanten-Admins sind in der folgenden Tabelle zu sehen und können dort verwaltet werden.

© 2015 SEPPmail AG

| User ID | E-Mail | Remove from this customer |
|---|---|---|
| Zeigt die Benutzer ID des jeweiligen Administrators, wie sie unter Users 203 angezeigt wird. | Zeigt die E-Mail Adresse des jeweiligen Administrators, wie sie unter Users 203 angezeigt wird. | Beinhaltet die Schaltfläche Remove zum Entfernen des jeweiligen Mandantenadmins. |

Die weitere Tabelle der Sektion dient dem Zuordnen weiterer Mandanten-Admins.

| Name | Assign to this customer |
|---|---|
| Beherbergt das DropDown Menü zur Auswahl des Benutzers, der als Mandanten-Admin zugeordnet werden soll. | Über die Schaltfläche Assign wird der unter **Name** ausgewählte Benutzer als Mandanten-Admin hinzugefügt. |

**Hinweis:**
Mandanten-Admins müssen über ein Passwort verfügen (siehe Benutzerdetails 204 User Data Password), damit das Anmelden am System möglich ist!

### Sektion Assigned managed domains

In dieser Sektion werden die dem Mandanten zugeordneten "Managed Domains" angezeigt. Die Zuordnung von "Managed Domains" zum Mandanten erfolgt in der Regel bereits bei der Anlage über das Menü Add/Edit Managed Domain 136.

| Domain name | Remove from this customer and reassign to Default Customer |
|---|---|
| Zeigt die zugeordnete(n) "Managed Domain(s)" | Beinhaltet die Schaltfläche Remove zum Entfernen der jeweiligen Managed Domain. |

Die folgende Tabelle wird nur dann angezeigt, wenn nicht zugeordnete "Managed Domains" vorhanden sind..

| Domain name | Assign to this customer |
|---|---|
| Beherbergt das DropDown Menü zur Auswahl der "Managed Domain", welche dem Mandanten zugeordnet werden soll. | Über die Schaltfläche Assign wird der unter *Domain name* ausgewählte Benutzer als Mandanten-Admin hinzugefügt. |

### Sektion Assigned GINA accounts

In dieser Sektion wird die Anzahl der dem Mandanten zugeordneten GINA-Benutzer angezeigt. Über die Schaltfläche Manage accounts können die GINA-Benutzer des Mandanten verwaltet sowie gegebenenfalls nicht zugeordnete Accounts zugeordnet werden (siehe Manage GINA accounts 226).

© 2015 SEPPmail AG

**Sektion Backup**

Die Schaltfläche **Download** startet das Herunterladen der Mandanten-Backup-Datei. Diese Datei beinhaltet ausschliesslich Konfiguration und Schlüsselmaterial des Mandanten der SEPPmail-Appliance. Voraussetzung für den Download des Backups ist die Vergabe eines Backup Passwortes, welches via **Change Password** gesetzt beziehungsweise geändert werden kann.
Soll ein Backup in die Appliance zurückgespielt werden, so erfolgt dies durch klicken von **Import Backup File**. Hierfür wird das zum Zeitpunkt der Erstellung des Backups gültige Backup-Passwort benötigt.

**Hinweis:**
Die in der Sektion **Customer details** unter **Customer Admin E-mail** eingetragen Adresse erhält täglich die Mandanten-Sicherung per E-Mail zugesandt. Voraussetzung ist natürlich ein gesetztes Backup Passwort.

#### 7.21.1.1 Manage GINA accounts

**Sektion Assigned GINA accounts**

Zeigt die dem Mandanten bereits zugeordneten GINA-Benutzer an und bietet die Möglichkeit einzelne GINA-Benutzer von diesem Mandanten zu entfernen, um diesen zum Beispiel einem anderen zuzuordnen. Somit bleibt das Schlüsselmaterial des GINA-Benutzers trotz dem Wechsel zu einem anderen Mandanten identisch.

| Name | E-Mail | Creation info | Remove from this customer |
|---|---|---|---|
| Zeigt den Namen des jeweiligen GINA-Benutzers, den er bei der Registrierung eingetragen hat. | Zeigt die E-Mail Adresse des jeweiligen GINA-Benutzers. | Zeigt<br>• wer gegebenenfalls die initiale GINA-E-Mail gesendet und somit den Benutzer generiert hat (Anzeige der E-Mail-Adresse bei unregistrierten, beziehungsweise "Created by..." bei bereits registrierten Benutzern)<br>• ob es sich um einen selbstregistrierten Benutzer handelt (Account...) | Beinhaltet die Schaltfläche **Remove** zum Entfernen GINA-Benutzers. |

**Sektion Assign other GINA accounts**

GINA-Benutzer, welche aktuell keinem Benutzer zugeordnet sind werden hier in zwei Tabellen angezeigt.

Dabei zeigt die erste Tabelle diejenigen GINA-Benutzer, welche dem Mandanten zwar nicht zugeordnet sind, jedoch von einem internen Benutzer der SEPPmail-Appliance erzeugt wurden, dessen E-Mail Domäne (Managed Domain) dem Mandanten zugeordnet ist.
In der Regel sollten solche GINA-Benutzer dem Mandanten mittels Schaltfläche **Assign** zugeordnet werden.

© 2015 SEPPmail AG

| Name | E-Mail | Creation info | Assign to this customer |
|---|---|---|---|
| Zeigt den Namen des jeweiligen GINA-Benutzers, den er bei der Registrierung eingetragen hat. | Zeigt die E-Mail Adresse des jeweiligen GINA-Benutzers. | Zeigt wer die initiale GINA-E-Mail gesendet und somit den Benutzer generiert hat. Dies ist immer ein interner Benutzer einer Managed Domain des Mandanten. | Beinhaltet die Schaltfläche **Assign** mit welcher der GINA-Benutzer dem Mandanten zugeordnet werden kann. |

Die zweite Tabelle der Sektion zeigt diejenigen GINA-Benutzer, welche keinem Mandanten zugeordnet sind und

a) von einem internen Benutzer der SEPPmail-Appliance erzeugt wurden, dessen E-Mail Domäne (Managed Domain) nicht dem Mandanten zugeordnet ist
b) mittels Selbstregistrierung (siehe ) generiert wurden.

In der Regel sollten GINA-Benutzer, welche von einem internen Benutzer der SEPPmail-Appliance einer "Managed Domain" eines anderen Mandanten erzeugt wurden, nicht zugeordnet werden.

| Name | E-Mail | Creation info | Assign to this customer |
|---|---|---|---|
| Zeigt den Namen des jeweiligen GINA-Benutzers, den er bei der Registrierung eingetragen hat. | Zeigt die E-Mail Adresse des jeweiligen GINA-Benutzers. | Zeigt, ob es sich um einen selbst registrierten GINA-Benutzer handelt, beziehungsweise wer die initiale GINA-E-Mail gesendet und somit den Benutzer generiert hat. Dies ist kein Benutzer einer Managed Domain des Mandanten. | Beinhaltet die Schaltfläche **Assign** mit welcher der GINA-Benutzer dem Mandanten zugeordnet werden kann. |

© 2015 SEPPmail AG

# 8 Referenz der Regelwerk-Anweisungen

## 8.1 Allgemeine Informationen

**Syntax**

Abschluss von Befehlen
Befehle müssen grundsätzlich mit einem Semicolon (;) abgeschlossen werden.

Parameter
Parameter werden immer in durch einfache Anführungszeichen ' ' begrenzt.
Parameter in eckigen Klammern, wie zum Beispiel [oldrecipient] sind optional und müssen nicht angegeben werden. Fehlt dieser Parameter wird in der Regel ein vordefinierter Standardwert bzw. Standardverhalten angewendet.
Eingabe Beispiele:

command([optional], required);
Eingabe command(‘’, ‘required’);
oder command(‘required’);

command(required, [optional], [optional]);
Eingabe command(‘required’);
oder command(‘required’, ‘’, ‘’);
oder command(‘required’, ‘’, ‘optional’);

Reguläre Ausdrücke
Innerhalb von Befehlen werden zum Teil reguläre Ausdrücke (regular expressions) verwendet, welche der Perl Systax entsprechen müssen.
Zahlreiche Erklärungen und Beispiele hierzu sind im Internet zu finden, beispielsweise unter
http://de.wikipedia.org/wiki/Regul%C3%A4rer_Ausdruck
http://wiki.selfhtml.org/wiki/Perl/Regul%C3%A4re_Ausdr%C3%BCcke

Verwenden von Anführungszeichen in Strings
Werden doppelte Anführungszeichen innerhalb eines Strings verwendet, so sind diese innerhalb der einfachen Anführungszeichen zu schreiben, also ' " " '.
Sind einfache Anführungszeichen innerhalb eines Strings zu schreiben, so sind diese durch doppelte Anführungszeichen zu begrezen, also " ' ' "

Variablen
Grundsätzlich stehen innerhalb von Vorlagen folgende Variablen zur Verfügung:

| Variable | Beschreibung |
|---|---|
| $header_from | liefert den Wert (Absender-Adresse) des "from headers" zurück. |
| $from | liefert den Absender aus dem "envelope" zurück. |
| $header_to | liefert den Wert (Empfänger-Adresse) des "to headers" zurück. |
| $to | liefert den Empfänger aus dem "envelope" zurück. |
| $header_cc | liefert den Wert (Empfänger-Adresse) des "cc headers" zurück. |

© 2015 SEPPmail AG

| Variable | Beschreibung |
|---|---|
| $mailid | liefert die eindeutige Message ID der E-Mail aus dem header zurück. |
| $subject | liefert den Betreff der E-Mail aus den "subject header" zurück. |

© 2015 SEPPmail AG

## 8.2 Kontrollstrukturen - if/else Anweisungen

Die `if/else` Anweisungen sind Kontrollstrukturen und dienen innerhalb des Rulesets der Ablaufsteuerung. Sie sind ein elementarer Bestandteil des Regelwerks. Ist eine Bedingung erfüllt, wird eine Aktionen ausgeführt, sonst wird eine alternative Aktion ausgeführt. Die auszuführende Aktion kann immer nur ein Befehl sein. Wenn als Aktion mehrere Befehle ausgeführt werden sollen, so können diese einzelnen Befehle in einem Anweisungsblock zusammengefasst werden. Ein Anweisungsblock wird innerhalb geschweifter Klammern geschrieben.

Mit `if` wird festgelegt, welche Voraussetzung zur Ausführung einer Aktion erfüllt sein muss. Mit `else` wird eine alternative Aktion eingeleitet, sollte die durch `if` geforderte Bedingung nicht erfüllt sein. Eine `if/else` Anweisung muss nicht durch ein Semikolon abgeschlossen werden. `if/else` Anweisungen können geschachtelt werden.
Jede `if` Anweisung muss mit einem `else` abgeschlossen werden.

**Aufbau einer if/else Anweisung**

```
if (Bedingung) {
   Anweisungsblock 1;
} else {
}
```

oder

```
if (Bedingung) {
   Anweisungsblock 1;
} else {
   Anweisungsblock 2;
}
```

Die `if`-Anweisung bestimmt aufgrund des Rückgabewertes der `Bedingung` den weiteren Verlauf im Programmablauf. Die Bedingung besteht aus einem einzelnen Befehl, welcher mindestens einen Rückgabewert hat.
`Anweisungsblock 1` wird nur dann ausgeführt, wenn der Rückgabewert ***positiv*** ist.
Anderenfalls wird - falls vorhanden - ausschliesslich `Anweisungsblock 2` ausgeführt.

**Beispiel**

```
if (authenticated()) {
} else {
   createaccount('@CREATEGPGKEYS@');
   log(1, 'user account generated');
}
```

**Erklärung**
Das Beispiel wertet den Rückgabewert des Befehls `authenticated()` aus. Konnte der interne interne Absender der E-Mail erfolgreich authentifiziert werden, so ist der Rückgabewert ***true***.
Nachdem für diesen Fall keine weitere Anweisung definiert wurde, wird ohne weitere Aktion im Programmablauf fortgefahren. Schlug die Authentifizierung fehl, das heisst der Rückgabewert ist **false**, so kommt der unter `else` angeführte Anweisungsblock zu tragen. Im Beispiel würde somit ein Benutzerkonto für den Absender angelegt und ein openPGP Schlüsselpaar erzeugt.

© 2015 SEPPmail AG

## 8.3 Allgemeine Befehle

### 8.3.1 add_rcpt()

Der Befehl `add_rcpt()` fügt der E-Mail eine zusätzliche Empfänger E-Mail-Adresse im Envelope hinzu.

**Aufbau des Befehls**

```
add_rcpt('e-mMail-address');
```

**Rückgabewert**

***positiv*** immer

**Parameter**

**e-mail-address**
Dieser Parameter definiert die E-Mail-Adresse welche dem Envelope als zusätzlicher Empfänger hinzugefügt werden soll.

**Beispiel**

```
add_rcpt('recipient@customer.org');
```

**Erklärung**
In diesem Beispiel wird der Empfänger "recipient@customer.org" hinzugefügt. Beim Empfänger erscheint die E-Mail im Posteingang so, als ob diese via BCC gesendet wurde. Der ursprüngliche Empfänger wird nicht verändert.

© 2015 SEPPmail AG

### 8.3.2 authenticated()

Der Befehl `authenticated()` überprüft den Identifikationsstatus des Absenders.

Der Identifikationsstatus des Absenders beinhaltet die Identität und die Authentifizierung.

**Aufbau des Befehls**

```
authenticated(['header']);
```

**Rückgabewert**

***positiv*** sofern der Absender erfolgreich authentifiziert werden konnte
***negativ*** bei Fehlschlagen der Authentifizierung des Absenders

**Hinweis:**
**Authentifiziert** bedeutet entweder, dass sich der Benutzer via SMTP authentifiziert hat, oder dass die E-Mail von einem E-Mail-Server kommt, der eine Relay-Berechtigung hat. Die Relay-Berechtigung ist im Menü **Mail System** 129 in der Sektion **Relaying** vorzunehmen.
Als Benutzer werden die lokalen "Named User" auf der Appliance bezeichnet (siehe **Users** 203).

**Parameter**

**header** (optional)
Wird `header` als Wert angegeben, so wird der Benutzer erneut mittels der im `FROM`-Feld des Headers der E-Mail enthaltenen E-Mail-Adresse authentifiziert. Im Standard wird die Adresse aus dem Envelope verwendet.

**Beispiel 1**

```
if (authenticated()) {
} else {
   createaccount('@CREATEGPGKEYS@');
   log(1, 'user account generated');
}
```

**Erklärung**
Das Beispiel wertet den Rückgabewert des Befehls `authenticated()` aus. Konnte der interne interne Absender der E-Mail erfolgreich authentifiziert werden, so ist der Rückgabewert ***true***. Nachdem für diesen Fall keine weitere Anweisung definiert wurde, wird ohne weitere Aktion im Programmablauf fortgefahren. Schlug die Authentifizierung fehl, das heisst der Rückgabewert ist **false**, so kommt der unter `else` angeführte Anweisungsblock zu tragen. Im Beispiel würde somit ein Benutzerkonto für den Absender angelegt und ein openPGP Schlüsselpaar erzeugt.

**Beispiel 2**

```
if (authenticated('header')) {
} else {
   createaccount('@CREATEGPGKEYS@');
   log(1, 'user account generated');
}
```

**Erklärung**
Dieses Beispiel wertet den Rückgabewert des Befehls `authenticated()` aufgrund des `FROM`-Feldes des Headers aus. Konnte der interne interne Absender der E-Mail aufgrund des Eintrags im `FROM`-Feld erfolgreich authentifiziert werden, so ist der Rückgabewert ***true***. Nachdem für diesen Fall keine weitere Anweisung definiert wurde, wird ohne weitere Aktion im Programmablauf

© 2015 SEPPmail AG

fortgefahren. Schlug die Authentifizierung fehl, das heisst der Rückgabewert ist **false**, so kommt der unter `else` angeführte Anweisungsblock zu tragen. Im Beispiel würde somit ein Benutzerkonto für den Absender angelegt und ein openPGP Schlüsselpaar erzeugt.

© 2015 SEPPmail AG

### 8.3.3 compare()

Der Befehl `compare()` prüft Werte in Headerfeldern auf einen zu definierenden Vergleichswert.

Dieser Befehl vergleicht den Inhalt eines Headers (`header-field`) mit Hilfe eines Vergleichsoperators (`operator`) mit einem angegebenen Wert (`value`)..

**Aufbau des Befehls**

```
compare('header-field', 'operator', 'value');
```

**Rückgabewert**

***positiv*** bei zutreffender Bedingung
***negativ*** bei nicht zutreffender Bedingung

**Parameter**

**header-field**
Gibt das Kopfzeilen-Feld an, dessen Inhalt gegen den Inhalt des Parameters `value` vergleichen werden soll. Als Kopfzeilen-Felder können alle Header in einer E-Mail verwendet werden.
Mögliche Werte

- return-path
- date
- from
- sender
- reply-to
- to
- cc
- bcc
- subject
- beliebiger x-header

**operator**
Mögliche Werte

- equal — vergleicht auf Gleichheit
- match — prüft auf das Zutreffen eines regulären Ausdrucks
- substitute — ist gleich wie `match`, entfernt aber den zutreffenden Teil von `value` aus `header-field`

**Hinweis:**
Codierte Felder werden vor dem Vergleich decodiert. Die Sonderzeichen Tabulator, Wagenrücklauf, Zeilenvorschub und Seitenende werden vor einem Vergleich mit dem Operator `equal` entfernt.

**value**
Gibt den Wert an, gegen den Vergleichen werden soll. Dieser Wert kann auch ein regulärer Ausdruck sein.

**Beispiel 1**

```
compare('x-smenc', 'equal', 'yes');
```

**Erklärung**

© 2015 SEPPmail AG

Dieses Beispiel prüft, ob das Header-Field `x-smenc` exakt den Wert `yes` beinhaltet. Dies bedeutet nicht, dass der Wert `yes` lediglich vorhanden ist, sondern, dass der Wert ausschliesslich `yes` beinhaltet.

**Beispiel 2**

```
if (compare('to', 'match', '\@cusomer\.com')) {
   tagsubject('[nosign]');
} else {}
```

**Erklärung**
Dieses Beispiel prüft bei einer ausgehenden E-Mail im Header-Field `to` mit dem Operator `match` auf das Vorhandensein der Domain `@customer.com` innerhalb der Empfänger E-Mail-Adresse. Wenn die E-Mail-Adresse des Empfängers die Zeichenkette `@customer.com` enthält, dann ist der Rückgabewert von `compare()` ***true***, im Betreff wird das das Tag `[nosign]` hinzugefügt. Je nach Basiskonfiguration des Rulesets wird dadurch das Signieren der E-Mail unterdrückt.

**Beispiel 3**

```
compare('subject', 'substitute', '(\s)*\[secure\]');
```

**Erklärung**
Dieses Beispiel prüft den Betreff (Header-Feld `subject`) einer E-Mail auf das Vorhandensein der Zeichenkette [secure] (als regulärer Ausdruck `(\s)*\[secure\]`). Wird diese Zeichenkette innerhalb des Betreff gefunden, so wird diese entfernt.

© 2015 SEPPmail AG

### 8.3.4 compareattr()

Der Befehl `compareattr()` prüft Attribute/Systemvariablen auf einen zu definierenden Vergleichswert.

Dieser Befehl vergleicht den Inhalt einer Variablen (`attribute`) mit Hilfe eines Vergleichsoperators ( `operator`) mit einem angegebenen Wert (`value`)..

**Aufbau des Befehls**

```
compareattr('attribute', 'operator', 'value');
```

**Rückgabewert**

***positiv*** bei zutreffender Bedingung
***negativ*** bei nicht zutreffender Bedingung

**Parameter**

**attribute**
`attribute` kann die Variable `connect_from` adressieren oder Variablen, die mit `ldap_read()` (siehe **ldap_read** 288) oder `setuserattr()` (siehe **setuserattr** 256) geschrieben wurden.

**operator**
Mögliche Werte

- equal vergleicht auf Gleichheit.
- match prüft auf das Zutreffen eines regulären Ausdrucks.

**value**
Wert gegen den verglichen werden soll.

**Beispiel**

```
if (compareattr('connect_from','equal','172.16.161.1')) {
     log(1,'Message comes from 172.16.161.1');
} else {
     log(1,'Message does NOT come from 172.16.161.1');
}
```

**Erklärung**
In diesem Beispiel wird überprüft, ob die zu verarbeitende E-Mail von einem E-Mail-Server bestimmten Server kommt. Es wird die Systemvariable `connect_from` ausgewertet.

© 2015 SEPPmail AG

### 8.3.5 comparebody()

Der Befehl `comparebody()` prüft den Nachrichtentext der E-Mail auf Vorhandensein einer Zeichenkette.

Dieser Befehl durchsucht den Nachrichtentext einer E-Mail nach dem angegebenen Wert (`value`).

**Aufbau des Befehls**

```
comparebody('value');
```

**Rückgabewert**

***positiv*** sofern der Wert aus value wenigstens einmal im Nachrichtentext vorkommt
***negativ*** sofern der Wert aus value nicht im Nachrichtentext vorkommt

**Parameter**

**value**
Der Parameter `value` definiert den Suchbegriff, nach dem innerhalb der E-Mail gesucht wird. `value` hat das Format eines regulären Ausdrucks.

**Beispiel**

```
if (comparebody('(\d{1,3}\.){3}\d{1,3}')) {
     log(1, 'Mail contains an IP address');
} else {
     log(1, 'Mail does not contain an IP address');
}
```

**Erklärung**
In diesem Beispiel wird innerhalb des Nachrichtentextes einer E-Mail auf das Vorhandensein einer IP-Adresse geprüft. Wird mindestens eine IP-Adresse gefunden, so wird der Log-Eintrag 'Mail contains an IP address' im System-Logger geschrieben. Wird keine IP-Adresse gefunden, so wird der Log-Eintrag 'Mail does not contain an IP address' im System-Logger geschrieben.

© 2015 SEPPmail AG

### 8.3.6 disclaimer()

Der Befehl `disclaimer()` fügt einen Textanhang einer bestehenden E-Mail hinzu.

Dieser Befehl fügt einen Textanhang aus dem angeführten Vorlage (`template`) einer bestehenden E-Mail hinzu. Wird keine Vorlage angegeben, so wird versucht, anhand der Einstellungen der **Managed Domains** den richtigen Disclaimer zu wählen. Dazu werden die den jeweiligen E-Mail Domänen zugeordneten Disclaimer ausgewertet.

**Aufbau des Befehls**

```
disclaimer(['template'], ['position'], ['force']);
```

Dieser Befehl fügt einen Textanhang aus dem angeführten `template` einer bestehenden E-Mail hinzu. Wenn eine leere Zeichenfolge als `template` angegeben ist, wird versucht, anhand der Einstellungen der **Managed Domains** den richtigen Disclaimer zu wählen. Dazu werden die den jeweiligen E-Mail Domänen zugeordneten Disclaimer ausgewertet.

**Rückgabewert**

***positiv*** immer

**Parameter**

**template** (optional)
Definiert den Namen der Vorlage (`template`), welche als Textanhang verwendet werden soll. Fussnoten- (Disclaimer-)Vorlagen werden über die Administrationsoberfläche (siehe **Mail Processing** 147 **Edit Disclaimer**) konfiguriert und verwaltet.
Wird keine Vorlage angegeben, so wird das [default] Disclaimer Template verwendet.

**position** (optional)
Mögliche Werte

- top oberhalb des E-Mail-Body
- bottom unterhalb des E-Mail-Body

default ist `bottom`

**force** (optional)
Dieser Paramater erzwingt das Hinzufügen eines Textanhangs an eine ausgehende E-Mail. Das heisst der Textanhang wird auch an Antwort-E-Mail angehängt.
Mögliche Werte:

- true, yes oder 1
- false, no oder 0

default ist 0

**Beispiel**

```
disclaimer('', 'bottom', 'yes');
```

**Erklärung**
In diesem Beispiel wird der Standard Textanhang anhand der Einstellungen innerhalb der **Managed Domains** ausgewählt und am Ende jeder versendeten E-Mail angehängt. Es ist dabei unerheblich, ob es sich um eine Antwort-E-Mail handelt oder nicht.

© 2015 SEPPmail AG

### 8.3.7 from_managed_domain()

Der Befehl `from_managed_domain()` prüft, ob eine E-Mail von einem Absender einer **Managed Domain** stammt.

#### Aufbau des Befehls

```
from_managed_domain();
```

#### Rückgabewert

***positiv*** sofern die E-Mail von einem Absender einer Managed Domain (siehe Mail System 129 Managed Domains) stammt

***negativ*** falls die E-Mail von einer anderen E-Mail Domäne stammt.

#### Parameter

keine

#### Beispiel

```
if (from_managed_domain()) {
     log('1', 'E-Mail is from managed domain');
} else {
     log('1', "E-Mail isn't from managed domain");
}
```

**Erklärung**
In diesem Beispiel wird geprüft, ob eine E-Mail von einer unter Managed Domains eingetragenen Absender E-Mail-Adresse gesendet wurde.

© 2015 SEPPmail AG

### 8.3.8 incoming()

Der Befehl `incoming()` bestimmt das Auslieferungsziel (intern/extern) einer E-Mail.

Dieser Befehl prüft, ob eine E-Mail lokal ausgeliefert wird. Sind nicht alle Empfänger der E-Mail *ausschliesslich lokal* oder *ausschliesslich extern*, so werden zwei Gruppen gebildet.

**Aufbau des Befehls**

```
incoming();
```

**Rückgabewert**

***positiv*** für die Gruppe der lokalen Empfänger
***negativ*** für die Gruppe der externen Empfänger

**Hinweis:**
Als lokale Empfänger werden diejenigen bezeichnet, deren E-Mail-Domänen auf der Appliance als **Managed Domains** definiert sind.
Alle anderen Empfänger werden als extern bezeichnet.

**Parameter**

keine

**Beispiel**

```
if (incoming()) {
     .
     Ruleset-Anweisungen für alle E-Mails die lokal zugestellt werden
können
     .
     Anweisungsblock 1 - Rückgabewert: positiv
     .
} else {
     .
     Ruleset-Anweisungen für alle E-Mails die extern zugestellt werden
müssen
     .
     Anweisungsblock 2  - Rückgabewert: negativ
}
```

**Erklärung**

In diesem Beispiel wird für eine eingehende E-Mail der `Anweisungsblock 1` ausgeführt. Für eine ausgehende E-Mail wird der `Anweisungsblock 2` ausgeführt.

© 2015 SEPPmail AG

### 8.3.9 log()

Der Befehl `log()` Erzeugt eiunen Eintrag im System-Log.

Der Eintrag im System-Log zeigt einen frei definierbaren Text (`description`) sowie eine Gewichtung (`severity`) des Eintrags. Weiterhin wird dem Eintrag in Spitzklammern die Message-ID aus dem E-Mail Header hinzugefügt. Die Aufgezeichneten Log-Meldungen können im Menü **Logs** eingesehen werden.

**Aufbau des Befehls**

```
log('severity', 'description');
```

**Rückgabewert**

***positiv*** immer

**Parameter**

**severity**
Dieser Parameter gibt die Gewichtung des Log-Eintrags an.

| severity | Bedeutung |
|---|---|
| 0 | debug |
| 1 | info |
| 2 | notice |
| 3 | warning |
| 4 | error |
| 5 | critical |
| 6 | alert |
| 7 | emergency |

**description**
Beschreibung wie Sie im System Log aufgezeichnet werden soll.

**Beispiel**

```
log('1', 'Hello World');
```

Header der E-Mail:

```
Date: Fri, 05 Aug 2013 11:40:00 +0200
From: sender@customer.com
To: recipient@customer.de
Subject: Some Topic
Content-Type: text/plain;
Message-Id: <E0D4DE42-DCB5-11D7>
```

Aufzeichnung im Log:

```
Aug 05 11:40:04 test gateway: <E0D4DE42-DCB5-11D7> Hello World
```

**Erklärung**
Die Zeichenkette (`description`) 'Hello World' wird mit der Gewichtung (`info`) im System Log aufgezeichnet.

© 2015 SEPPmail AG

### 8.3.10 logheader()

Der Befehl `logheader()` schreibt den Inhalt des genannten Headers oder x-header in das System-Log.

Dieser Befehl dient im Regelfall dem Debuggen der Verarbeitung von E-Mails durch die RuleEngine. Die Aufgezeichneten Log-Meldungen können im Menü **Logs** eingesehen werden.

**Aufbau des Befehls**

```
logheader('header');
```

**Rückgabewert**

***positiv*** immer

**Parameter**

**header**
Angabe des zu protokollierenden Headers oder X-Headers.
Mögliche Werte

- return-path
- date
- from
- sender
- reply-to
- to
- cc
- bcc
- subject
- beliebiger x-header

**Beispiel**

```
logheader('Message-ID');
```

Header der E-Mail:

```
Date: Fri, 05 Aug 2013 11:40:00 +0200
From: sender@customer.com
To: recipient@customer.de
Subject: Some Topic
Content-Type: text/plain;
Message-Id: <E0D4DE42-DCB5-11D7>
```

Aufzeichnung im Log:

```
Aug 05 11:40:04 Message-Id: <E0D4DE42-DCB5-11D7>
```

**Erklärung**
Die Zeichenkette aus dem Header "Message-ID:" wird wie aufgezeigt im System Log aufgezeichnet.

© 2015 SEPPmail AG

### 8.3.11 logsubject()

Der Befehl `logsubject()` protokolliert den Inhalt der Betreffzeile einer E-Mail im System-Log.

Die Aufgezeichneten Log-Meldungen können im Menü **Logs** eingesehen werden.

**Aufbau des Befehls**

```
logsubject();
```

**Rückgabewert**
***positiv*** immer

**Parameter**
keine

**Beispiel**

```
logsubject();
```

Header der E-Mail:

```
Date: Fri, 05 Aug 2013 11:40:00 +0200
From: sender@customer.com
To: recipient@customer.de
Subject: Some Topic
Content-Type: text/plain;
Message-Id: <E0D4DE42-DCB5-11D7>
```

Aufzeichnung im Log:

```
Aug 05 11:40:04 Message Subject is Some Topic
```

**Erklärung**
Die Zeichenkette aus dem Header "Subject:" wird wie aufgezeigt im System Log aufgezeichnet.

© 2015 SEPPmail AG

### 8.3.12 normalize_header()

Der Befehl `normalize_header()` ersetzt alle Sonderzeichen in einem (X-)Header durch normale ASCII-Zeichen.

Dieser Befehl ersetzt alle Sonderzeichen des angegebenen Headers (`header`) durch normale ASCII-Zeichen. Sonderzeichen können zum Beispiel deutsche Umlaute wie ä, ö, ü aber auch ? sein.

**Aufbau des Befehls**

```
normalize_header('header');
```

**Rückgabewert**

***positiv*** immer

**Parameter**

**header**
Angabe des zu bearbeitenden Headers oder X-Headers an.
Mögliche Werte

- return-path
- date
- from
- sender
- reply-to
- to
- cc
- bcc
- subject
- beliebiger x-header

**Beispiel 1**

```
normalize_header('subject');
```

**Erklärung**
In diesem Beispiel wird im Header-Feld `subject` zum Beispiel aus der Zeichenkette "Herr Müller" die normalisierte Form "Herr Mueller".

**Beispiel 2**

```
normalize_header('to');
```

**Erklärung**
In diesem Beispiel wird im Header-Feld `to` aus der Zeichenkette
'<Bernd Hänsel> bernd.haensel@customer.com'
die normalisierte Form
'<Bernd Haensel> bernd.haensel@customer.com'.

© 2015 SEPPmail AG

### 8.3.13 notify()

Der Befehl `notify()` sendet eine E-Mail Benachrichtigung an einen zu definierenden Empfänger bei Verarbeitung einer anderen E-Mail.

Dieser Befehl erzeugt eine E-Mail Benachrichtigung an einen zu definierenden Empfänger ( `recipient`) unter Verwendung der Vorlage (`template`). Optional können `header` beziehungsweise `x-header` in diese Benachrichtigungs-E-Mail geschrieben werden.

**Aufbau des Befehls**

```
notify('recipient', 'template', ['header: value[;header: value]']);
```

**Rückgabewert**

***positiv*** immer

**Parameter**

**recipient**
Angabe der Empfänger-E-Mail-Adresse der Benachrichtigungs-E-Mail.
Mögliche Werte

- E-Mail-Adresse — Sendet eine Benachrichtigung an die angegebene SMTP-E-Mail-Adresse
- sender — Benachrichtigt den ursprünglichen Absender der E-Mail
- admin — Benachrichtigt den lokalen SEPPmail-Administrator
  Dieser wird im Menü **Mail System** in der Sektion **SMTP settings** unter **Postmaster address** definiert.

**template**
Dieser Parameter definiert die zu verwendende Vorlage für diese Benachrichtigungsmail.
Die Vorlage kann im Menü **Mail Processing** in der Sektion **Edit Email Templates** erstellt und verwaltet werden.

**header: value** (optional)
Angabe des zu schreibenden `header`s inklusive des zugehörigen Wertes `value`.
Mögliche Werte für `header`

- return-path:
- date:
- from:
- sender:
- reply-to:
- to:
- cc:
- bcc:
- subject:
- beliebiger x-header

**Hinweis:**
Das Setzen mehrerer `header` beziehungsweise x-`header` ist durch trennen mittels Semicolon möglich.

**Beispiel**

© 2015 SEPPmail AG

```
notify('sender', 'bounce_noenc', 'from: "System Admin"
<admin@meinefirma.ch>;subject: Benachrichtigung; x-MyOwnHeader: Test');
```

**Erklärung**
In diesem Beispiel wird eine Benachrichtigungs-E-Mail an den ursprünglichen Absender - welcher über die Variable `sender` zur Verfügung gestellt wird - generiert. Als Vorlage für die E-Mail wird das Standard Template `bounce_noenc` verwendet. Im `header` der Benachrichtigungs-E-Mail wird als Absender ""System Admin" <admin@meinefirma.ch>"  und als Betreff "Benachrichtigung" gesetzt. Weiterhin wird ein x-header mit der Bezeichnung "x-MyOwnHeader" und dem Wert "Test" geschrieben.

© 2015 SEPPmail AG

### 8.3.14 replace_rcpt()

Der Befehl `replace_rcpt()` ersetzt den oder die Empfänger einer E-Mail durch einen anzugebenden anderen.

Die Empfänger der zu verarbeitenden E-Mail können in Abhängigkeit der verwendeten Parameter verändert werden. Jeder Parameter entspricht einem regulären Ausdruck, der als Ergebnis eine E-Mail-Adresse oder einen Teil einer E-Mail-Adresse liefern muss.
Ebenfalls können Teile der beiden Parameter als regulärer Ausdruck beschrieben werden. So kann zum Beispiel nach dem Domainanteil innerhalb der Parameter gesucht werden und dieser durch einen neuen Wert ersetzt werden.
Mehrere Empfänger können durch Semikolon getrennt eingegeben werden.

**Aufbau des Befehls**

```
replace_rcpt(['oldrecipient',] 'newrecipient');
```

**Rückgabewert**

***positiv*** immer

**Parameter**

**oldrecipient** (optional)
Regulärer Ausdruck der die ursprügliche E-Mail-Adresse oder Teile davon beschreibt.

**newrecipient**
Regulärer Ausdruck der die neue E-Mail-Adresse oder Teile davon beschreibt.

**Beispiel 1**

```
replace_rcpt('support@customer.com');
```

**Erklärung**
In diesem Beispiel wird der ursprüngliche Empfänger der E-Mail durch den Empfänger " support@customer.com" ersetzt.
Wäre beispielsweise der ursprünglich Empfänger der E-Mail "admin@customer.com", so würde dieser entfernt und durch den neuen Empfänger (`newrecipient`) "support@customer.com" ersetzt. Somit wird die E-Mail an den neuen Empfänger "support@customer.com" gesendet.

**Beispiel 2**

```
replace_rcpt('@mydomain\.com', '@customer\.ch');
```

**Erklärung**
In diesem Beispiel wird im Parameter `oldrecipient` der Domainanteil der ursprünglichen E-Mail-Adresse des/der Empfänger/s von '@mydomain.com' in den Wert des Paramaters `newrecipient`, '@customer.ch', geändert. Der Bestandteil der E-Mail-Adresse vor dem '@' bleibt dabei unverändert. Falls `oldrecipient` angegeben wird, wird nur dieser Empfänger bzw. der Bestandteil des Empfängers angepasst.
Falls mehrere E-Mail-Empfängeradressen vorhanden sind, würden alle Empfängeradressen von '@mydomain.com' zu '@mydomain.ch' geändert werden.

© 2015 SEPPmail AG

### 8.3.15 replace_sender()

Der Befehl replace_sender() verändert den Absender im Envelope einer E-Mail.

Dieser Befehl ersetzt den ursprünglichen Absender einer E-Mail im Envelope durch einen Anderen ( `newsender`). Der Wert des Headers `from` wird dadurch nicht verändert.
Weiterhin können auch Teile der Absenderadresse über reguläre Ausdrücke (Parameter `subst`) manipuliert werden.

**Aufbau des Befehls**

```
replace_sender('newsender', ['subst']);
```

**Rückgabewert**

***positiv*** immer

**Parameter**

**newsender**
Dieser Parameter ist der Wert, durch den die ursprüngliche Absender E-Mail-Adresse im Envelope ersetzt wird. Ist der Parameter `subst` mit angegeben, so ist `newsender` die Zeichenkette, die für den Teil der E-Mail-Adresse eingesetzt wird auf den `subst` zutrifft.

**subst** (optional)
Regulärer Ausdruck der auf die ursprüngliche Absender E-Mail-Adresse angewendet wird.

**Beispiel 1**

```
replace_sender('new_sender@customer.com');
```

**Erklärung**
In diesem Beispiel wird die E-Mail-Adresse im Envelope der E-Mail durch ' new_sender@customer.com' ersetzt.

**Beispiel 2**

```
replace_sender('@customer.com', '\@customer\.org');
```

**Erklärung**
In diesem Beispiel wird der Teil die E-Mail-Adresse im Envelope der E-Mail durch auf den regulären Ausdruck '\@customer\.org' zutrifft durch '@customer.com' ersetzt.

© 2015 SEPPmail AG

### 8.3.16 rmatch()

Der Befehl `rmatch()` prüft, ob ein regulärer Ausdruck auf mindestens einen Empfänger im Envelope zutrifft.

**Aufbau des Befehls**

```
rmatch('regexp');
```

**Rückgabewert**

***positiv*** wenn der reguläre Ausdruck (`regexp`) auf mindestens einen Empfänger zutrifft
***negativ*** wenn der reguläre Ausdruck (`regexp`) auf keinen Empfänger zutrifft

**Parameter**

**regexp**
Definiert den regulären Ausdruck der verglichen werden soll.

**Beispiel 1**

```
if (rmatch('\@customer\.org')) {
     notify ('sender', 'info_send_email');
} else {
}
```

**Erklärung**
In diesem Beispiel wird überprüft, ob die E-Mail-Adresse mindestens eines Empfängers einer E-Mail den Domain-Bestandteil '@customer.org' hat. Ist dies der Fall, dann wird eine E-Mail Benachrichtigung an den Absender gesendet.

© 2015 SEPPmail AG

### 8.3.17 rmatchsplit()

Der Befehl `rmatch()` prüft, ob ein regulärer Ausdruck auf mindestens einen Empfänger im Envelope zutrifft und teilt die Mail in zwei Gruppen

Über diesem Befehl wird im Envelope einer E-Mail auf das Vorhandensein eines regulären Ausdrucks (`regexp`) geprüft. Eine E-Mail wird bei Bedarf in zwei Gruppen aufgeteilt: Eine Gruppe, mit Empfängern, welche dem  dem regulären Ausdruck entsprechen und eine weitere Gruppe dessen Empfänger den regulären Ausdruck nicht enthalten. Somit wird der Befehl `rmatchsplit()` klassisch innerhalb der `if/else` Kontrollstruktur verwendet.

**Aufbau des Befehls**

```
rmatchsplit('regexp');
```

**Rückgabewert**

***positiv*** für die Gruppe, deren Empfänger den regulären Ausdruck `regexp` enthalten
***negativ*** für die Gruppe, deren Empfänger den regulären Ausdruck `regexp` nicht enthalten

**Parameter**

**regexp**
Dieser Parameter definiert den regulären Ausdruck auf dessen Vorhandensein innerhalb der E-Mail geprüft wird.

**Beispiel**

```
if (rmatchsplit('sales@customer\.com|invoice')) {
     log(1, 'regex test successful');
} else {
     log(1, 'regex test not successful');
}
```

**Erklärung**
In diesem Beispiel wird die E-Mail auf das Vorhandensein des Ausdrucks `sales@customer.com` oder `invoice` geprüft. Wird einer dieser Textbestandteile innerhalb des Envelope der E-Mail gefunden, so wird die Anweisung `log(1, 'regex test successful')` ausgeführt, sonst wird die Anweisung `log(1, 'regex test not successful')` ausgeführt.

© 2015 SEPPmail AG

### 8.3.18 rmheader()

Der Befehl `rmheader()` löscht eine Header oder X-Header Zeile innerhalb einer E-Mail.

**Aufbau des Befehls**

```
rmheader('header');
```

**Rückgabewert**

***positiv*** immer

**Parameter**

**header**

Angabe des zu löschenden Headers oder X-Headers an.

Mögliche Werte

- return-path
- date
- from
- sender
- reply-to
- to
- cc
- bcc
- subject
- beliebiger x-header

**Hinweis:**
Falls mehrere Header mit dem unter `header` angegebenen Namen existieren, werden alle zutreffenden Header gelöscht.

**Beispiel**

```
rmheader('X-Greylist');
```

**Erklärung**

In diesem Beispiel werden alle `X-Greylist` Header entfernt.

© 2015 SEPPmail AG

### 8.3.19 setheader()

Der Befehl `setheader()` fügt eine Header-Zeile innerhalb einer E-Mail hinzu oder verändert eine vorhandene.

**Aufbau des Befehls**

```
setheader('header', 'value');
```

**Rückgabewert**

***positiv*** immer

**Parameter**

**header**
Angabe des Headers oder X-Headers der hinzugefügt oder geändert werden soll.
Mögliche Werte

- return-path
- date
- from
- sender
- reply-to
- to
- cc
- bcc
- subject
- beliebiger x-header

**Hinweis:**
Falls mehrere Header mit dem unter `header` angegebenen Namen existieren, wird der jeweils erste gefundene Header angepasst.

**value**
Angabe des Wertes, den der Header annehmen soll.

**Beispiel 1**

```
setheader('x-smenc','yes');
```

**Erklärung**
In diesem Beispiel wird einer E-Mail der zusätzliche Header `x-smenc` mit dem Wert 'yes' hinzugefügt.

**Beispiel 2**

```
setheader('from','info@customer.com');
```

**Erklärung**
In diesem Beispiel wird in einer E-Mail das Header-Feld `from` auf dem Wert 'info@customer.com' geändert.

© 2015 SEPPmail AG

### 8.3.20 tagsubject()

Der Befehl `tagsubject()` fügt dem Betreff einer E-Mail den zu definierenden Text hinzu.

**Aufbau des Befehls**

```
tagsubject('text');
```

**Rückgabewert**

***positiv*** immer

**Parameter**

**text**
Der Parameter gibt den Text (Zeichenkette) an, der am Ende der Betreffzeile angehängt wird.

**Beispiel**

```
tagsubject('[priv]');
```

**Erklärung**
In diesem Beispiel wird an den Inhalt der Betreffzeile einer E-Mail die Zeichenkette '[priv]' am Ende angehängt.

### 8.3.21 tag_subject()

Der Befehl `tag_subject()` wurde durch `tagsubject()` (siehe tagsubject 253) ersetzt und ist nicht länger gültig.

© 2015 SEPPmail AG

# 8.4 Befehle für die Benutzerverwaltung

## 8.4.1 createaccount()

Der Befehl `createaccount()` erstellt neue Benutzerkonten.

Als Benutzerkonto wird ein lokales SEPPmail Benutzerkonto bezeichnet. Dieses Benutzerkonto kann im Menü **Users** eingesehen werden.

**Aufbau des Befehls**

```
createaccount(['keys'],['userID'],['name']);
```

**Rückgabewert**

***positiv*** immer

**Parameter**

**keys** (optional)
Dieser Parameter gibt an, welches Schlüsselmaterial beim Erstellen der Benutzerkontos automatisch generiert werden soll. Das Format entspricht einer Bitmaske in Oktalnotation. Wird der Parameter nicht angegeben, so wird kein Schlüsselmaterial erzeugt.
Die folgenden Werte stehe zur Verfügung:

Bit 0 : openPGP-Schlüsselpaar generieren
Bit 1 : S/MIME-Zertifikat mit der eigenen CA generieren
Bit 2 : S/MIME-Zertifikat via CA-Connector generieren

| | Mask | | | | |
|---|---|---|---|---|---|
| Bit 0: openPGP | x | x | x | | |
| Bit 1: S/MIME mit eigener CA | | x | | | x |
| Bit 2: S/MIME via CA-Connector | | | x | x | |
| Wert für `keys` | 1 | 3 | 5 | 4 | 2 |

**userID** (optional)
Dieser Parameter gibt die eindeutige ID des Benutzers an.
Wird dieser Parameter nicht angegeben, so wird für das Generieren des Benutzers seine E-Mail Adresse als `userID` verwendet.

**name** (optional)
Dieser Parameter gibt des Namen des Benutzers an.
Wird dieser Parameter nicht angegeben, so wird für das Generieren des Benutzers der Anzeigename, beziehungsweise wenn dieser nicht vorhanden ist seine E-Mail Adresse als `name` verwendet.

**Hinweis:**

- Für `userID` und `name` können Variablen benutzt werden, die durch den Befehl `ldap_read()` gesetzt wurden.
- Sonderzeichen in `userID` und `name` werden automatisch ersetzt.

© 2015 SEPPmail AG

### 8.4.2 member_of()

Der Befehl `member_of()` prüft die zugehörigkeit eines Absenders zu einer Gruppe.

Als Gruppe wird eine lokale SEPPmail Gruppe bezeichnet. Diese Gruppen werden im Menü **Groups** verwaltet.

#### Aufbau des Befehls

```
member_of('group');
```

#### Rückgabewert

***positiv*** wenn der Absender der angegebenen Gruppe zugeordnet ist
***negativ*** wenn der Absender nicht der angegebenen Gruppe zugeordnet ist

#### Parameter

**group**
Definiert den Namen der Gruppe auf dessen Mitgliedschaft die E-Mail-Adresse des Absenders geprüft werden soll.

#### Beispiel

```
if (member_of('support')) {
     setheader('x-smenc','yes');
} else {}
```

**Erklärung**
In diesem Beispiel wird geprüft, ob der Absender Mitglied der Gruppe 'support' ist. Falls ja, dann wird als Rückgabewert ***true*** geliefert, und der Befehl `setheader()` wird ausgeführt. Falls nein wird als Rückgabewert ***false*** geliefert.

© 2015 SEPPmail AG

### 8.4.3 setuserattr()

Der Befehl `setuserattr()` fügt einem Benutzerkonto Attribute hinzu oder ändert diese.

Das Benutzerkonto kann im Menü **Users** eingesehen werden.

**Aufbau des Befehls**

```
setuserattr('attr', 'value');
```

**Rückgabewert**
***positiv*** immer

**Parameter**

**ATTR und VALUE**
Folgende Systemattribute (**attr**) stehen mit den jeweiligen Werten (**value**) gemäss folgender Tabelle zur Verfügung:

<table>
<tr><th>ATTR</th><th>VALUE</th></tr>
<tr><td>accountOptions</td><td>Bit 0: User darf nicht verschlüsseln<br>Bit 1: nicht belegt<br>Bit 2: User darf nicht signieren<br><br><table><tr><th></th><th colspan="3">Mask</th></tr><tr><td>Bit 0: User darf nicht verschlüsseln</td><td>x</td><td></td><td>x</td></tr><tr><td>Bit 1: nicht belegt</td><td>-</td><td>-</td><td>-</td></tr><tr><td>Bit 2: User darf nicht signieren</td><td></td><td>x</td><td>x</td></tr><tr><td>Wert für <code>value</code></td><td>1</td><td>4</td><td>5</td></tr></table></td></tr>
<tr><td>SN</td><td>Name des Benutzers</td></tr>
<tr><td>UID</td><td>User ID</td></tr>
</table>

**Hinweis:**

- Für `value` können Variablen benutzt werden, die durch `ldap_read()` gesetzt wurden.
- Es können alle Attribute von InetOrgPerson benutzt werden.
- Die Attribute können in der Administrationsoberfläche angezeigt werden.

Das Alleinstellungsmerkmal eines SEPPmail Benutzerkontos ist die E-Mail Adresse, weshalb diese auch nicht geändert werden kann.

© 2015 SEPPmail AG

## 8.5 Befehle für die Zertifikatsverwaltung

### 8.5.1 attachpgpkey()

Der Befehl `attachpgpkey()` hängt den openPGP-Public-Key des Absenders (User) an eine E-Mail an.

Dieser Befehl hängt den openPGP-Public-Key des Absenders (interner Benutzer in der Appliance aus dem Menü **Users**) an eine E-Mail als Dateianhang an, um diesen dem Empfänger bereit zu stellen.

**Aufbau des Befehls**

```
attachpgpkey();
```

**Rückgabewert**

***positiv*** immer

**Parameter**

keine

### 8.5.2 has_smime_key()

Der Befehl `has_smime_key()` prüft, ob der Benutzer einen gültigen privaten S/MIME-Schlüssel besitzt.

Dieser Befehl prüft, ob ein Benutzer (interner Benutzer in der Appliance aus dem Menü **Users**) einen gültigen privaten S/MIME-Schlüssel besitzt.

**Aufbau des Befehls**

```
has_smime_key();
```

**Rückgabewert**

***positiv*** wenn der Benutzer einen gültigen privaten S/MIME-Schlüssel besitzt

***negativ*** wenn der Benutzer

- keine oder nur abgelaufene S/MIME-Schlüssel besitzt.
- auf den Status **may not encrypt** gesetzt ist.
- auf den Status **may not sign** gesetzt ist.

**Parameter**

keine

© 2015 SEPPmail AG

### 8.5.3 smime_create_key()

Der Befehl `smime_create_key()` erstellt ein S/MIME-Zertifikat für einen internen Benutzer durch die lokale CA.

**Aufbau des Befehls**

```
smime_create_key(['subject']);
```

**Rückgabewert**

***positiv*** immer

**Parameter**

**subject** (optional)
Definiert das Subject für das zu erzeugende S/MIME-Zertifikat.
Innerhalb der `subject`-Zeichenkette steht die Variable `$sender` zur Verfügung, welch in die E-Mail Adresse des Absenders aufgelöst wird.
Wird kein Parameter angegeben, so wird als `subject` der "Static Subject Part" aus der internen CA (siehe CA 185 **Internal CA Settings** **Static Subject Part**) und die E-Mail Adresse des Absenders eingetragen.

**Beispiel**

```
smime_create_key('/C=CH/OU=Department/O=Company/emailAddress=$sender');
```

**Erklärung**
In diesem Beispiel wird ein S/MIME-Zertifikat über die lokale CA generiert, in welchem das optionale `subject` mitgegeben wird.

© 2015 SEPPmail AG

# 8.6 Befehle für das Handhaben von Nachrichten

## 8.6.1 archive()

Der Befehl `archive()` kopiert die E-Mail und stellt sie einen zusätzlichen Empfänger zu.

Die E-Mail wird innerhalb der Verarbeitung kopiert und in einem neuen Envelope der zusätzlich angegebenden E-Mail Adresse (`e-mail-address`) zugestellt (vergleiche **Mail Processing** 147 **Ruleset Generator** Archiving).

**Aufbau des Befehls**

```
archive('e-mail-address');
```

**Rückgabewert**

***positiv*** immer

**Parameter**

**e-mail-address** (optional)
E-Mail Adresse des zusätzlichen Empfängers.

**Beispiel**

```
archive('recipient@customer.com');
```

**Erklärung**
In diesem Beispiel wird die gerade verarbeitete E-Mail zusätzlich an den Empfänger ' recipient@customer.com' gesendet.

© 2015 SEPPmail AG

### 8.6.2 bounce()

Der Befehl `bounce()` verweigert das Annehmen einer E-Mail.

Dieser Befehl erzeugt eine Bounce-E-Mail und löscht die ursprüngliche E-Mail. Das Aussehen der Bounce-E-Mail wird durch eine Vorlage definiert. Der Absender dieser Bounce-E-Mail ist **admin**. Optional wird der Header der ursprünglichen E-Mail der Bounce-E-Mail als Dateianlage angehängt.

**Hinweis:**

- Alle nachfolgenden Befehle werden ignoriert.
- Dieser Befehl kann nicht die Bedingung einer `if/else` Anweisung sein (siehe Abschnitt **Kontrollstrukturen - if/else Anweisungen** 230).

**Aufbau des Befehls**

```
bounce('template', ['attachheader']);
```

**Rückgabewert**

kein

**Parameter**

**template**
Definiert die zu verwendende Vorlage.
Vorlagen werden über die Administrationsoberfläche (siehe Mail Processing 147 **Edit Mail Templates**) definiert und verwaltet.

**attach_header**
Dieser Parameter gibt an, ob der Header der ursprünglichen E-Mail der Bounce-E-Mail als Dateianlage angehängt werden soll (`true`) oder nicht (`false`).
Mögliche Werte:

- true, yes oder1
- false, no oder 0

default ist 0

**Beispiel**

```
bounce('bounce', 'yes');
```

**Erklärung**
Die Auslieferung der E-Mail soll verhindert werden. Zugleich sollen dem Absender über eine Rück-(Bounce-)E-Mail Informationen zur Verfügung gestellt werden. Der Inhalt dieser Rück-E-Mail ist in der Vorlage `bounce` definiert. Weiterhin wird der Header der nicht ausgelieferten E-Mail als Anlage angehängt (Wert `yes` des Parameters `attach_header`).

© 2015 SEPPmail AG

### 8.6.3 deliver()

Der Befehl `deliver()` ermöglicht es, eine E-Mail unmittelbar auszuliefern.

**Hinweis:**
- Alle nachfolgenden Befehle werden ignoriert.
- Dieser Befehl kann nicht die Bedingung einer `if/else` Anweisung sein (siehe Abschnitt Kontrollstrukturen - if/else Anweisungen 230).

**Aufbau des Befehls**

```
deliver(['mailserver[:port]'|'loop'|'queueless']);
```

**Rückgabewert**

***positiv*** immer

**Parameter**

Wird kein Parameter angegeben, so wird die E-Mail dem lokalen Mail-Transport-Agent (MTA) übergeben.

**mailserver** (optional)
Gibt den E-Mail Server an, über welchen die E-Mail ausgeliefert werden soll.
Wird kein Parameter angegeben, so wird die E-Mail dem lokalen Mail-Transport-Agent (MTA) übergeben.

**:port** (optional)
Gibt den Port an, auf welchem der angegeben E-Mail Server E-Mails empfängt.
Standard ist Port 25 SMTP

**loop** (optional)
Die E-Mail wird an den E-Mail Server zurückgegeben, von welchem sie angenommen wurde.

**queueless** (optional)
Diese Einstellung bewirkt, dass E-Mails an einzelne Empfänger während der Verarbeitung nicht zwischengelagert werden. Stattdessen wird die eingehende Verbindung erst quittiert, wenn dieabgehende Verbindung quittiert wurde. Wenn beim Versand an mehrere Empfänger die Annahme für einige Empfänger nicht quittiert wird, befinden sich diese E-Mails kurzzeitig bis zur Quittierung durch die empfangenden E-Mail Server auf der Appliance.

**Hinweis:**
Die Parameter
- **mailserver[:port]**,
- **loop**,
- **queueless**

schliessen sich gegenseitig aus.

**Beispiel 1**

```
deliver('relay.customer.com:587');
```

**Erklärung**
In diese Beispiel wird die E-Mail an den angegebenen E-Mail Server mit dem Ziel-Port TCP/587 gesendet.

**Beispiel 2**

```
deliver();
```

**Erklärung**
In diesem Beispiel wird die E-Mail direkt über den eigenen lokalen E-Mail-Transport-Agent (MTA)

© 2015 SEPPmail AG

ausgeliefert.

© 2015 SEPPmail AG

### 8.6.4 drop()

Der Befehl `drop()` weist eine E-Mail mit dem angegebenen SMTP-Code und einen frei definierbarem Informationstext zurück.

**Hinweis:**

- Alle nachfolgenden Befehle werden ignoriert.
- Dieser Befehl kann nicht die Bedingung einer `if/else` Anweisung sein (siehe Abschnitt Kontrollstrukturen - if/else Anweisungen 230).

**Aufbau des Befehls**

```
drop(['smtp-code'], ['text']);
```

.

**Rückgabewert**

***positiv*** immer

**Parameter**

**smtp-code** (optional)
Der `smtp-code` gibt den Grund für das Zurückweisen einer E-Mail an.
**Default:**Wird dieser Parameter nicht angegeben, so wird der Code "555" verwendet.
Die Bedeutung der Codes gliedert sich wie folgt:

| | |
|---|---|
| 1XX | Mailserver hat die Anforderung akzeptiert, ist aber selbst noch nicht tätig geworden. Eine Bestätigungsmeldung ist erforderlich. |
| 2XX | Mailserver hat die Anforderung erfolgreich ohne Fehler ausgeführt. |
| 3XX | Mailserver hat die Anforderung verstanden, benötigt aber zur Verarbeitung weitere Informationen. |
| 4XX | Mailserver hat einen temporären Fehler festgestellt. Wenn die Anforderung ohne jegliche Änderung wiederholt wird, kann die Verarbeitung möglicherweise abgeschlossen werden. |
| 5XX | Mailserver hat einen fatalen Fehler festgestellt. Die Anforderung kann nicht verarbeitet werden. |

Quelle: Wikipedia
Detaillierte Auflistungen der Fehlercodes sind zum Beispiel unter http://www.supermailer.de/smtp_reply_codes.htm zu finden.

**text** (optional)
Der Informations`text` spezifiziert den Grund des Abweisens näher.
**Default:**Wird dieser Parameter nicht angegeben, so wird der Text "mail NOT accepted" ausgegeben.

**Beispiel**

```
drop('451', 'Die Nachricht konnte nicht entschluesselt werden');
```

**Erklärung**
In diesem Beispiel wird eine E-Mail mit dem `smtp-code` 451 "Requested action aborted: local error in processing" und dem zusätzlichen Hinweis`text` "Die Nachricht konnte nicht entschluesselt werden" zurückgewiesen.

© 2015 SEPPmail AG

### 8.6.5 reprocess()

Der Befehl `reprocess()` ermöglicht es, eine oder mehrere E-Mail(s) erneut zu verarbeiten.

Alle an eine E-Mail angehängten E-Mails - oder auch openPGP verschlüsselten Dateien - werden erneut verarbeitet und an den Absender zurückgesendet. Dies kann dann erforderlich sein, wenn sich im Posteingang eines Benutzers noch verschlüsselte E-Mails befinden. Diese E-mails können als Anhang einer neuen E-Mail des betroffenen Benutzers zur erneuten Verarbeitung - also zum entschlüsseln - an die Appliance gesendet werden.
Der Befehl hat keinen Rückgabewert. Dieser Befehl hat keinen Parameter.

**Hinweis:**

- Die ursprüngliche Message-ID wird aus den neu entschlüsselten E-Mails entfernt.
- Es wird keine Bounce E-Mail an den Absender erzeugt.
- Alle nachfolgenden Befehle werden ignoriert.
- Dieser Befehl kann nicht die Bedingung einer `if/else` Anweisung sein (siehe Abschnitt **Kontrollstrukturen - if/else Anweisungen** 230).

**Aufbau des Befehls**

```
reprocess();
```

**Rückgabewert**
kein

**Parameter**
keine

**Beispiel**

```
if (compare('to', 'match', '(?i)reprocess\@decrypt\.reprocess')) {
     log(1, 'reprocess recipient found - Re-injecting attached
messages');
     reprocess();
     drop('220', 'message reprocessed');
} else {
}
```

**Erklärung**
Sendet ein interner Benutzer (eine) verschlüsselte E-Mail(s) als Anhang in einer neuen, nicht verschlüsselten E-Mail an die systemspezifische E-Mail-Adresse `reprocess@decrypt.reprocess`,so werden die E-Mails aus dem Anhang erneut verarbeitet. Somit wird versucht diese anhängenden E-Mails zu entschlüsseln. Für den Vorgang werden entsprechende Log-Einträge erzeugt. Nach dem Ausführen von `reprocess()` wird die ursprüngliche, neue E-Mail mit `drop()` gelöscht.

© 2015 SEPPmail AG

# 8.7 Befehle für kryptographische Behandlung

## 8.7.1 openPGP

### 8.7.1.1 pgp_encrypted()

Der Befehl `pgp_encrypted()` prüft, ob eine E-Mail openPGP verschlüsselt ist.

Dieser Befehl prüft, ob eine E-Mail openPGP verschlüsselt ist. Dabei spielt die Art der Verschlüsselung (Domänen oder Benutzer basiert) keine Rolle.

**Aufbau des Befehls**

```
pgp_encrypted();
```

**Rückgabewert**

***positiv*** wenn die E-Mail openPGP verschlüsselt ist
***negativ*** wenn die E-Mail nicht openPGP verschlüsselt ist

**Parameter**

keine

**Beispiel**

| Zeile | Code |
|---|---|
| 01 | `if (pgp_encrypted()) {` |
| 02 | `  log(1, 'e-mail is pgp encrypted');` |
| 03 | `  if (decrypt_domain_pgp() {` |
| 04 | `  log(1, 'email successfully pgp domain decrypted');` |
| 05 | `  } else {` |
| 06 | `  log(1, 'email could not be pgp domain decrypted');` |
| 07 | `  if (decrypt_pgp() {` |
| 08 | `  log(1, 'email successfully pgp decrypted');` |
| 09 | `  } else {` |
| 10 | `  log(1, 'email could not be pgp decrypted');` |
| 11 | `  }` |
| 12 | `  }` |
| 13 | `} else {` |
| 14 | `  log(1, 'e-mail is not pgp encrypted');` |
| 15 | `}` |

**Erklärung**

In diesem Beispiel wird zunächst geprüft, ob eine E-Mail openPGP verschlüsselt ist (Zeile 1) und ein entsprechender ein Log Eintrag geschrieben (Zeile 2 und 14). Ist die E-Mail openPGP verschlüsselt, so wird zunächst versucht die E-Mail mit dem privaten openPGP Domänen Schlüssel zu entschlüsseln (Zeile 3) und Erfolg beziehungsweise Misserfolg protokolliert wird (Zeile 4 und 6).
Konnte nicht mit dem privaten open PGP Domänen Schlüssel entschlüsselt werden, so wird nun versucht mit einem Benutzer basierten, privaten open PGP Schlüssel zu entschlüsseln (Zeile 7). Das Ergebnis dieser Aktion wird ebenfalls protokolliert (Zeile 8 und 10).

© 2015 SEPPmail AG

### 8.7.1.2 Domänen basiert

#### 8.7.1.2.1 decrypt_domain_pgp()

Der Befehl `decrypt_domain_pgp()` entschlüsselt openPGP Domänen verschlüsselte E-Mails.

Dieser Befehl versucht eingehende openPGP Domänen verschlüsselten Texte und Anlagen einer E-Mail zu entschlüsseln, die durch den Absender mittels öffentlichen openPGP Domänen Schlüssel (siehe **Mail System** **Add/Edit Managed Domain** 136 **openPGP Domain Encryption**) verschlüsselt wurden.

**Aufbau des Befehls**

```
decrypt_domain_pgp();
```

**Rückgabewert**

***positiv*** wenn mindestens ein Text oder eine Anlage entschlüsselt werden wurde
***negativ*** wenn das Entschlüsseln fehlgeschlagen ist.

**Parameter**

keine

**Beispiel**

| Zeile | Code |
|---|---|
| 01 | `if (decrypt_domain_pgp() {` |
| 02 | `log(1, 'email successfully pgp domain decrypted');` |
| 03 | `} else {` |
| 04 | `log(1, 'email could not be pgp domain decrypted');` |
| 05 | `}` |

**Erklärung**

In diesem Beispiel wird eine openPGP Domänen verschlüsselte E-Mail entschlüsselt (Zeile 1). Erfolg beziehungsweise Misserfolg des Entschlüsselns wird protokolliert (Zeile 2 und 4).

© 2015 SEPPmail AG

8.7.1.2.2 domain_pgp_keys_avail()

Der Befehl `domain_pgp_keys_avail()` prüft die Verfügbarkeit von öffentlichen openPGP Domänen Schlüsseln.

Dieser Befehl prüft die Verfügbarkeit öffentlicher openPGP Domänen Schlüssel (siehe **Domain Certificates** 221 **openPGP Domain Keys**) der Empfänger für das Verschlüsseln ausgehender E-Mails.

**Aufbau des Befehls**

```
domain_pgp_keys_avail();
```

**Rückgabewert**

***positiv*** für die Gruppe mit vorhandenem öffentlichen openPGP Domänen Schlüssel
***negativ*** für die Gruppe ohne öffentlichen openPGP Domänen Schlüssel

**Parameter**

keine

**Beispiel**

| Zeile | Code |
|---|---|
| 01 | `if (domain_pgp_keys_avail(){` |
| 02 | `log(1, 'pgp domain key available');` |
| 03 | `if (encrypt_domain_pgp() {` |
| 04 | `log(1, 'email successfully pgp domain encrypted');` |
| 05 | `} else {` |
| 06 | `log(1, 'email could not be pgp domain encrypted');` |
| 07 | `}` |
| 08 | `} else {` |
| 09 | `log(1, 'no pgp domain key available');` |
| 10 | `}` |

**Erklärung**

In diesem Beispiel wird zunächst geprüft, ob ein passender öffentlicher openPGP Domänen Schlüssel für das Verschlüsseln zur Verfügung steht (Zeile 1). Das Ergebnis dieser Abfrage wird protokolliert (Zeile 2 und 9). Steht ein entsprechender Schlüssel zur Verfügung, wird mit dem Verschlüsseln fortgefahren (Zeile 3), dessen Erfolg beziehungsweise Misserfolg ebenfalls protokolliert wird (Zeile 4 und 6).

© 2015 SEPPmail AG

8.7.1.2.3 encrypt_domain_pgp()

Der Befehl `encrypt_domain_pgp()` verschlüsselt E-Mails mittels openPGP Domänen Verschlüsselung.

Dieser Befehl verschlüsselt alle Texte und Anlagen ausgehender E-Mails via openPGP Domänen Verschlüsselung. Dabei wird das openPGP-Inline Verfahren genutzt.
Stehen nicht für alle Empfänger der E-Mail Domäne öffentliche openPGP Domänen Schlüssel (siehe Domain Certificates 221 **openPGP Domain Keys**) für das Verschlüsseln bereit, so werden zwei Gruppen gebildet.

**Aufbau des Befehls**

```
encrypt_domain_pgp();
```

**Rückgabewert**

***positiv*** für die Gruppe der Empfänger, für die verschlüsselt werden konnte
***negativ*** für die Gruppe der Empfänger, bei denen das Verschlüsseln nicht möglich gewesen ist

**Parameter**

keine

**Beispiel**

| Zeile | Code |
|---|---|
| 01 | `if (encrypt_domain_pgp() {` |
| 02 | `log(1, 'email successfully pgp domain encrypted');` |
| 03 | `} else {` |
| 04 | `log(1, 'email could not be pgp domain encrypted');` |
| 05 | `}` |

**Erklärung**

In diesem Beispiel wird versucht eine E-Mail mittels öffentlichen openPGP Domänen Schlüssel des Kommunikationspartners zu Verschlüsseln (Zeile 1). Erfolg beziehungsweise Misserfolg der Aktion wird protokolliert (Zeile 2 und 4).

© 2015 SEPPmail AG

### 8.7.1.3 Benutzer basiert

#### 8.7.1.3.1 decrypt_pgp()

Der Befehl `decrypt_pgp()` entschlüsselt openPGP verschlüsselte E-Mails.

Dieser Befehl versucht alle openPGP verschlüsselten Texte und Anlagen einer eingehenden E-Mail zu entschlüsseln, die durch den Absender mittels des persönlichen öffentlichen openPGP Schlüssels des Empfängers (siehe **Users** **Benutzerdetails** 204) verschlüsselt wurden.

**Aufbau des Befehls**

```
decrypt_pgp();
```

**Rückgabewert**

***positiv*** wenn mindestens ein Text oder eine Anlage entschlüsselt werden konnte
***negativ*** wenn das Entschlüsseln fehlgeschlagen ist.

**Parameter**

keine

**Beispiel**

| Zeile | Code |
|---|---|
| 01 | `if (decrypt_pgp() {` |
| 02 | `log(1, 'email successfully pgp decrypted');` |
| 03 | `} else {` |
| 04 | `log(1, 'email could not be pgp decrypted');` |
| 05 | `}` |

**Erklärung**

In diesem Beispiel wird eine Benutzer basiert openPGP verschlüsselte E-Mail entschlüsselt (Zeile 1). Erfolg beziehungsweise Misserfolg des Entschlüsselns wird protokolliert (Zeile 2 und 4).

© 2015 SEPPmail AG

8.7.1.3.2 pgp_keys_avail()

Der Befehl `pgp_keys_avail()` prüft die Verfügbarkeit von öffentlichen openPGP Schlüsseln.

Dieser Befehl prüft die Verfügbarkeit personenbezogener öffentlicher openPGP Schlüssel der Empfänger (siehe **openPGP public keys** 216) für das Verschlüsseln ausgehender E-Mails.

**Aufbau des Befehls**

```
pgp_keys_avail();
```

**Rückgabewert**

***positiv*** für die Gruppe mit vorhandenem öffentlichen openPGP Schlüssel
***negativ*** für die Gruppe ohne öffentlichen openPGP Schlüssel

**Parameter**

keine

**Beispiel**

| Zeile | Code |
|---|---|
| 01 | `if (pgp_keys_avail(){` |
| 02 | `log(1, 'pgp key available');` |
| 03 | `if (encrypt_pgp() {` |
| 04 | `log(1, 'email successfully pgp encrypted');` |
| 05 | `} else {` |
| 06 | `log(1, 'email could not be pgp encrypted');` |
| 07 | `}` |
| 08 | `} else {` |
| 09 | `log(1, 'no pgp key available');` |
| 10 | `}` |

**Erklärung**

In diesem Beispiel wird zunächst geprüft, ob ein passender, Benutzer basierter öffentlicher openPGP Schlüssel für das Verschlüsseln zur Verfügung steht (Zeile 1). Das Ergebnis dieser Abfrage wird protokolliert (Zeile 2 und 9). Steht ein entsprechender Schlüssel zur Verfügung, wird mit dem Verschlüsseln fortgefahren (Zeile 3), dessen Erfolg beziehungsweise Misserfolg ebenfalls protokolliert wird (Zeile 4 und 6).

© 2015 SEPPmail AG

8.7.1.3.3 encrypt_pgp()

Der Befehl `encrypt_pgp()` ermöglicht es, E-Mails via openPGP zu verschlüsseln und zu signieren.

Dieser Befehl verschlüsselt alle Texte und Anlagen einer ausgehenden E-Mail mit dem öffentlichen openPGP Schlüssel des Empfängers (siehe **openPGP public keys** 216). Dabei wird das openPGP-Inline Verfahren genutzt. Optional kann zusätzlich mit dem privaten openPGP Schlüssel des Absenders (siehe **Users** **Benutzerdetails** 204) signiert werden.
Stehen nicht für alle Empfänger öffentliche openPGP Schlüssel bereit, so werden zwei Gruppen gebildet.

**Aufbau des Befehls**

```
encrypt_pgp(['sign'], ['address']);
```

**Rückgabewert**

***positiv*** für die Gruppe der Empfänger, für die verschlüsselt werden konnte, unabhängig ob das optionale Signieren erfolgreich war

***negativ*** für die Gruppe der Empfänger, bei denen das Verschlüsseln nicht möglich gewesen ist

**Parameter**

**sign**
Dieser Parameter entscheidet, ob die E-Mail mit dem privaten openPGP Schlüssel des Absenders signiert werden soll.
Mögliche Werte:

- true, yes oder1
- false, no oder 0

default ist 0

**address**
E-Mail-Adresse des Empfängers, dessen öffentlicher openPGP Schlüssel für das Verschlüsseln verwendet werden soll.
Wird kein Parameter angegeben, so wird der öffentliche openPGP Schlüssel des jeweiligen Empfängers verwendet.

**Beispiel**

```
encrypt_pgp('yes', 'recipient@customer.org');
```

**Erklärung**
In diesem Beispiel wird versucht alle Texte und Anlagen einer E-Mail zu verschlüsseln und zu signieren, da der Parameter `sign` den Wert 'yes' hat. Für das Verschlüsseln wird der öffentliche openPGP Schlüssel des durch den Parameter `address` spezifizierten Empfängers verwendet. Im Beispiel 'recipient@customer.org'.

© 2015 SEPPmail AG

## 8.7.2 S/MIME

### 8.7.2.1 smime_encrypted()

Der Befehl `smime_encrypted()` prüft, ob eine E-Mail S/MIME verschlüsselt ist.

**Aufbau des Befehls**

```
smime_encrypted();
```

**Rückgabewert**

***positiv*** wenn die E-Mail S/MIME verschlüsselt ist
***negativ*** wenn die E-Mail nicht S/MIME verschlüsselt ist

**Parameter**

keine

**Beispiel**

| Zeile | Code |
|---|---|
| 01 | `if (smime_encrypted()) {` |
| 02 | `  log(1, 'e-mail is S/MIME encrypted');` |
| 03 | `  if (decrypt_domain_smime() {` |
| 04 | `  log(1, 'email successfully S/MIME domain decrypted');` |
| 05 | `  } else {` |
| 06 | `  log(1, 'email could not be S/MIME domain decrypted');` |
| 07 | `  if (decrypt_smime() {` |
| 08 | `  log(1, 'email successfully S/MIME decrypted');` |
| 09 | `  } else {` |
| 10 | `  log(1, 'email could not be S/MIME decrypted');` |
| 11 | `  }` |
| 12 | `  }` |
| 13 | `} else {` |
| 14 | `  log(1, 'e-mail is not S/MIME encrypted');` |
| 15 | `}` |

**Erklärung**

In diesem Beispiel wird zunächst geprüft, ob eine E-Mail S/MIME verschlüsselt ist (Zeile 1) und ein entsprechender ein Log Eintrag geschrieben (Zeile 2 und 14). Ist die E-Mail S/MIME verschlüsselt, so wird zunächst versucht die E-Mail mit dem privaten S/MIME Domänen Schlüssel zu entschlüsseln (Zeile 3) und Erfolg beziehungsweise Misserfolg protokolliert wird (Zeile 4 und 6). Konnte nicht mit dem privaten S/MIME Domänen Schlüssel entschlüsselt werden, so wird nun versucht mit einem Benutzer basierten, privaten S/MIME Schlüssel zu entschlüsseln (Zeile 7). Das Ergebnis dieser Aktion wird ebenfalls protokolliert (Zeile 8 und 10).

© 2015 SEPPmail AG

### 8.7.2.2 Domänen basiert

#### 8.7.2.2.1 decrypt_domain_smime()

Der Befehl `decrypt_domain_smime()` entschlüsselt S/MIME Domänen verschlüsselte E-Mails.

Dieser Befehl versucht eingehende S/MIME Domänen verschlüsselte E-Mails zu entschlüsseln, die durch den Absender mittels öffentlichen S/MIME Domänen Schlüssel (siehe **Mail System** Add/Edit Managed Domain 136 **S/MIME Domain Encryption**) verschlüsselt wurden.

**Aufbau des Befehls**

```
decrypt_domain_smime();
```

**Rückgabewert**

***positiv*** wenn die E-Mail entschlüsselt werden konnte
***negativ*** wenn das Entschlüsseln der E-Mail fehlgeschlagen ist.

**Parameter**

keine

**Beispiel**

| Zeile | Code |
|---|---|
| 01 | `if (decrypt_domain_smime() {` |
| 02 | `log(1, 'email successfully S/MIME domain decrypted');` |
| 03 | `} else {` |
| 04 | `log(1, 'email could not be S/MIME domain decrypted');` |
| 05 | `}` |

**Erklärung**

In diesem Beispiel wird eine S/MIME Domänen verschlüsselte E-Mail entschlüsselt (Zeile 1). Erfolg beziehungsweise Misserfolg des Entschlüsselns wird protokolliert (Zeile 2 und 4).

© 2015 SEPPmail AG

8.7.2.2.2 domain_smime_keys_avail()

Der Befehl `domain_smime_keys_avail()` prüft die Verfügbarkeit von öffentlichen S/MIME Domänen Schlüsseln (Zertifikaten).

Dieser Befehl prüft die Verfügbarkeit von Domänen Zertifikaten (siehe **Domain Certificates** 221 **SMIME Domain Certificates** beziehungsweise **Managed Domain Certificates**) der Empfänger für das Verschlüsseln ausgehender E-Mails.

**Aufbau des Befehls**

```
domain_smime_keys_avail();
```

**Rückgabewert**

***positiv*** für die Gruppe mit vorhandenem S/MIME Domänen Zertifikat
***negativ*** für die Gruppe ohne S/MIME Domänen Zertifikat

**Parameter**

keine

**Beispiel**

| Zeile | Code |
|---|---|
| 01 | `if (domain_smime_keys_avail(){` |
| 02 | `log(1, 'S/MIME domain certificate available');` |
| 03 | `if (encrypt_domain_smime() {` |
| 04 | `log(1, 'email successfully S/MIME domain encrypted');` |
| 05 | `} else {` |
| 06 | `log(1, 'email could not be S/MIME domain encrypted');` |
| 07 | `}` |
| 08 | `} else {` |
| 09 | `log(1, 'S/MIME domain certificate available');` |
| 10 | `}` |

**Erklärung**

In diesem Beispiel wird zunächst geprüft, ob ein passendes S/MIME Domänen Zertifikat das Verschlüsseln zur Verfügung steht (Zeile 1). Das Ergebnis dieser Abfrage wird protokolliert (Zeile 2 und 9). Steht ein entsprechender Schlüssel zur Verfügung, wird mit dem Verschlüsseln fortgefahren (Zeile 3), dessen Erfolg beziehungsweise Misserfolg ebenfalls protokolliert wird (Zeile 4 und 6).

© 2015 SEPPmail AG

8.7.2.2.3 encrypt_domain_smime()

Der Befehl `encrypt_domain_smime()` verschlüsselt E-Mails mittels S/MIME Domänen Verschlüsselung.

Dieser Befehl verschlüsselt die komplette ausgehende E-Mail via S/MIME Domänen Verschlüsselung. Davon ausgenommen sind lediglich E-Mail Header, da diese unter anderem für den E-Mail Transport benötigt werden.
Stehen nicht für alle Empfänger der E-Mail Domäne öffentliche S/MIME Domänen Schlüssel ( Zertifikate) für das Verschlüsseln bereit (siehe **Domain Certificates** 221 **SMIME Domain Certificates** beziehungsweise **Managed Domain Certificates**), so werden zwei Gruppen gebildet.

**Aufbau des Befehls**

```
encrypt_domain_smime();
```

**Rückgabewert**

***positiv*** für die Gruppe der Empfänger, für die verschlüsselt werden konnte
***negativ*** für die Gruppe der Empfänger, bei denen das Verschlüsseln nicht möglich gewesen ist

**Parameter**

keine

**Beispiel**

| Zeile | Code |
|---|---|
| 01 | `if (encrypt_domain_smime() {` |
| 02 | `log(1, 'email successfully S/MIME domain encrypted');` |
| 03 | `} else {` |
| 04 | `log(1, 'email could not be S/MIME domain encrypted');` |
| 05 | `}` |

**Erklärung**

In diesem Beispiel wird versucht eine E-Mail mittels S/MIME Domänen Zertifikat des Kommunikationspartners zu Verschlüsseln (Zeile 1). Erfolg beziehungsweise Misserfolg der Aktion wird protokolliert (Zeile 2 und 4).

© 2015 SEPPmail AG

### 8.7.2.3 Benutzer basiert

#### 8.7.2.3.1 decrypt_smime()

Der Befehl `decrypt_smime()` entschlüsselt S/MIME verschlüsselte E-Mails.

Dieser Befehl entschlüsselt eingehende E-Mails, welche durch den Absender mittels des persönlichen öffentlichen S/MIME Schlüssel (Zertifikat) des Empfängers (siehe **Users** **Benutzerdetails** 204) verschlüsselt wurden.

**Aufbau des Befehls**

```
decrypt_smime();
```

**Rückgabewert**

***positiv*** wenn die E-Mail entschlüsselt wurde
***negativ*** wenn das Entschlüsseln der E-Mail fehlgeschlagen ist.

**Parameter**

keine

**Beispiel**

| Zeile | Code |
|---|---|
| 01 | `if (decrypt_smime() {` |
| 02 | `log(1, 'email successfully S/MIME decrypted');` |
| 03 | `} else {` |
| 04 | `log(1, 'email could not be S/MIME decrypted');` |
| 05 | `}` |

**Erklärung**

In diesem Beispiel wird eine Benutzer basiert S/MIME verschlüsselte E-Mail entschlüsselt (Zeile 1). Erfolg beziehungsweise Misserfolg des Entschlüsselns wird protokolliert (Zeile 2 und 4).

© 2015 SEPPmail AG

8.7.2.3.2 smime_keys_avail()

Der Befehl `smime_keys_avail()` prüft die Verfügbarkeit von öffentlichen S/MIME Schlüsseln (Zertifikate).

Dieser Befehl prüft die Verfügbarkeit personenbezogener Zertifikate der Empfänger (siehe X.509 Certificates 217) für das Verschlüsseln ausgehender E-Mails.

**Aufbau des Befehls**

```
smime_keys_avail();
```

**Rückgabewert**

***positiv*** für die Gruppe mit vorhandenem S/MIME Zertifikat
***negativ*** für die Gruppe ohne S/MIME Zertifikat

**Parameter**

keine

**Beispiel**

| Zeile | Code |
|---|---|
| 01 | `if (smime_keys_avail(){` |
| 02 | `log(1, 'S/MIME certificate available');` |
| 03 | `if (encrypt_smime() {` |
| 04 | `log(1, 'email successfully S/MIME encrypted');` |
| 05 | `} else {` |
| 06 | `log(1, 'email could not be S/MIME encrypted');` |
| 07 | `}` |
| 08 | `} else {` |
| 09 | `log(1, 'no S/MIME certificate available');` |
| 10 | `}` |

**Erklärung**

In diesem Beispiel wird zunächst geprüft, ob ein passendes, Benutzer basiertes S/MIME Zertifikat für das Verschlüsseln zur Verfügung steht (Zeile 1). Das Ergebnis dieser Abfrage wird protokolliert (Zeile 2 und 9). Steht ein entsprechender Schlüssel zur Verfügung, wird mit dem Verschlüsseln fortgefahren (Zeile 3), dessen Erfolg beziehungsweise Misserfolg ebenfalls protokolliert wird (Zeile 4 und 6).

© 2015 SEPPmail AG

8.7.2.3.3 encrypt_smime()

Der Befehl `encrypt_smime()` verschlüsselt E-Mails mittels S/MIME Domänen Verschlüsselung.

Dieser Befehl verschlüsselt die komplette ausgehende E-Mail via S/MIME Verschlüsselung. Davon ausgenommen sind lediglich E-Mail Header, da diese unter anderem für den E-Mail Transport benötigt werden.
Stehen nicht für alle Empfänger der E-Mail personenbezogene öffentliche S/MIME Schlüssel ( Zertifikate) für das Verschlüsseln bereit (siehe **X.509 Certificates** 217), so werden zwei Gruppen gebildet.

**Aufbau des Befehls**

```
encrypt_smime();
```

**Rückgabewert**

***positiv*** für die Gruppe der Empfänger, für die verschlüsselt werden konnte
***negativ*** für die Gruppe der Empfänger, bei denen das Verschlüsseln nicht möglich gewesen ist

**Parameter**

keine

**Beispiel**

| Zeile | Code |
|---|---|
| 01 | `if (encrypt_smime() {` |
| 02 | `log(1, 'email successfully S/MIME encrypted');` |
| 03 | `} else {` |
| 04 | `log(1, 'email could not be S/MIME encrypted');` |
| 05 | `}` |

**Erklärung**

In diesem Beispiel wird versucht eine E-Mail mittels Benutzer basiertem S/MIME Zertifikat des Kommunikationspartners zu Verschlüsseln (Zeile 1). Erfolg beziehungsweise Misserfolg der Aktion wird protokolliert (Zeile 2 und 4).

© 2015 SEPPmail AG

8.7.2.3.4 smime_signed()

Der Befehl `smime_signed()` prüft, ob eine E-Mail S/MIME signiert ist.

**Aufbau des Befehls**

```
smime_signed();
```

**Rückgabewert**

***positiv*** wenn die E-Mail S/MIME signiert ist
***negativ*** wenn die E-Mail nicht S/MIME signiert ist

**Parameter**

keine

**Beispiel**

| Zeile | Code |
|---|---|
| 01 | `if (smime_signed()) {` |
| 02 | `log(1, 'e-mail is S/MIME signed');` |
| 03 | `if (validate_smime_sig('1') {` |
| 04 | `log(1, 'signature is valid');` |
| 05 | `} else {` |
| 06 | `log(1, 'signature is invalid');` |
| 07 | `}` |
| 08 | `} else {` |
| 09 | `log(1, 'e-mail is not S/MIME signed');` |
| 10 | `}` |

**Erklärung**

In diesem Beispiel wird zunächst geprüft, ob eine E-Mail S/MIME signiert ist (Zeile 1) und ein entsprechender ein Log Eintrag geschrieben (Zeile 2 und 9). Ist die E-Mail S/MIME signiert, so wird Signatur geprüft (Zeile 3) und Erfolg beziehungsweise Misserfolg protokolliert wird (Zeile 4 und 6).

© 2015 SEPPmail AG

#### 8.7.2.3.5 validate_smime_sig()

Der Befehl `validate_smime_sig()` prüft die S/MIME Signatur einer E-Mail auf ihre Gültigkeit.

**Aufbau des Befehls**

```
validate_smime_sig('fetch-certificate');
```

**Rückgabewert**

***positiv*** wenn folgende Bedingungen erfüllt sind:

- die E-Mail ist unverändert
- der Signatur-Schlüssel ist gültig, das heisst er
  - er stammt von einer als vertrauenswürdig eingestuften Certificate Authority (CA)
  - hat das Ablaufdatum noch nicht überschritten
  - ist auf keiner der Appliance bekannten Certificate Revocation List (CRL) aufgeführt

***negativ*** wenn eine der Bedingungen nicht erfüllt ist

**Parameter**

**fetch-certificate** (optional)
Dieser Parameter gibt an, ob bei der in der Signatur enthaltene öffentliche Schlüssel (Zertifikat) des Absenders gespeichert werden soll (siehe **X.509 Certificates** 217). Gespeichert werden nur Zertifikate, deren Zertifikatskette bekannt ist (siehe **X.509 Root Certificates** 218). Dies unabhängig davon, ob die E-Mail verändert wurd oder nicht
Mögliche Werte:

- true, yes oder 1
- false, no oder 0

default ist 0

**Beispiel**

| Zeile | Code |
|---|---|
| 01 | `if (validate_smime_sig('1') {` |
| 02 | `log(1, 'signature is valid');` |
| 03 | `} else {` |
| 04 | `log(1, 'signature is invalid');` |
| 05 | `}` |

**Erklärung**
In diesem Beispiel wird die S/MIME Signatur einer E-Mail geprüft (Zeile 1) und Erfolg beziehungsweise Misserfolg protokolliert wird (Zeile 2 und 4).

© 2015 SEPPmail AG

8.7.2.3.6 delete_smime_sig()

Der Befehl `delete_smime_sig()` ermöglicht es, die S/MIME-Signatur einer E-Mail zu löschen.

Dieser Befehl löscht eine Signatur aus der signierten E-Mail.

**Hinweis:**
Die Gültigkeit der S/MIME-Signatur wird nicht geprüft.

**Aufbau des Befehls**

```
delete_smime_sig();
```

**Rückgabewert**

***positiv*** wenn die E-Mail S/MIME signiert war
***negativ*** wenn die E-Mail nicht S/MIME signiert war

**Parameter**

keine

**Beispiel**

| Zeile | Code |
|---|---|
| 01 | `if (validate_smime_sig('1') {` |
| 02 | `log(1, 'signature is valid');` |
| 03 | `delete_smime_sig();` |
| 04 | `} else {` |
| 05 | `log(1, 'signature is invalid');` |
| 06 | `}` |

**Erklärung**
In diesem Beispiel wird die S/MIME Signatur einer E-Mail geprüft (Zeile 1) und Erfolg beziehungsweise Misserfolg protokolliert wird (Zeile 2 und 5). Wurde die Signatur als gültig eingestuft, so wird sie gelöscht (Zeile 3).

© 2015 SEPPmail AG

8.7.2.3.7 sign_smime()

Der Befehl `sign_smime()` signiert eine E-Mail.

Dieser Befehl signiert die ausgehende E-Mail mit dem persönlichen privaten S/MIME Schlüssels des Absenders (siehe **Users** **Benutzerdetails** 204).

**Aufbau des Befehls**

```
sign_smime();
```

**Rückgabewert**

***positiv*** wenn die Nachricht erfolgreich signiert wurde
***negativ*** bei Fehlschlagen der Signatur

**Parameter**

keine

**Beispiel**

| Zeile | Code |
|---|---|
| 01 | `if (has_smime_key(){` |
| 02 | `log(1, 'S/MIME key available, trying to sign');` |
| 03 | `if (sign_smime() {` |
| 04 | `log(1, 'signing successful');` |
| 05 | `} else {` |
| 06 | `log(1, 'signing failed');` |
| 07 | `}` |
| 08 | `} else {` |
| 09 | `log(1, 'no S/MIME key available, do not sign');` |
| 10 | `}` |

**Erklärung**

In diesem Beispiel wird zunächst geprüft, ob ein privater S/MIME Schlüssel verfügbar ist (Zeile 1). Das Ergebnis wird protokolliert (Zeile 2 und 9). Ist ein privater S/MIME Schlüssel vorhanden, so wird versucht die E-Mail zu signieren (Zeile 3) und das Ergebnis dieser Aktion wird ebenfalls in das Log geschrieben (Zeile 4 beziehungsweise 6).

© 2015 SEPPmail AG

## 8.7.3 GINA

### 8.7.3.1 encrypt_webmail()

Der Befehl `encrypt_webmail()` verschlüsselt eine E-Mail unter Verwendung der GINA-Technologie.

Dieser Befehl verschlüsselt eine ausgehende Nachricht via GINA-Technologie an die Empfängeradresse.
Die Empfängeradresse wird aus der aktuell verarbeiteten Nachricht entnommen.
Nach dem verschlüsseln einer Nachricht mittels GINA-Technologie sollte diese immer direkt mit `deliver()` versendet werden.

**Aufbau des Befehls**

```
encrypt_webmail(['template']);
```

**Rückgabewert**

***positiv*** immer

**Parameter**

**template** (optional)
Definiert das angelegte GINA-Profil beziehungsweise die GINA-Domain.
Wird kein Parameter angegeben, so wird die Vorlage anhand der E-Mail-Domäne der Absenderadresse ausgewählt (siehe Mail System 129 Managed Domains **GINA Settings**)

**Beispiel**

| Zeile | Code |
|---|---|
| 01 | `if (encrypt_webmail() {` |
| 02 | `log(1, 'email successfully GINA encrypted');` |
| 03 | `deliver();` |
| 04 | `} else {` |
| 05 | `log(1, 'email could not be GINA encrypted');` |
| 06 | `drop('451', 'Die Nachricht konnte nicht verschluesselt` |
| 07 | `werden');` |
| | `}` |

**Erklärung**
In diesem Beispiel wird versucht eine E-Mail mittels <%OEM-WEBMAIL-GINA%-Technologie zu Verschlüsseln (Zeile 1). Erfolg beziehungsweise Misserfolg der Aktion wird protokolliert (Zeile 2 und 5). Bei erfolgreichem Verschlüsseln wird die E-Mail - wie empfohlen - direkt ausgeliefert (Zeile 3). Andernfalls wird sie mit dem temporären Fehler "451" und dem Hinweistext "Die Nachricht konnte nicht verschluesselt werden" abgewiesen (Zeile 6).

© 2015 SEPPmail AG

### 8.7.3.2 pack_mail()

Der Befehl `pack_mail()` ermöglicht das Senden von GINA-E-Mails über ein abgekoppeltes GINA-Relay-System.

Dieser Befehl ermöglicht das Senden von GINA-E-Mails über ein abgekoppeltes GINA-Relay-System (vergleiche **Mail Processing** 147 **Ruleset Generator** **Advanced Options** Use remote GINA server, reachable under the following email address).

**Aufbau des Befehls**

```
pack_mail('e-mail-address', ['domainsignature']);
```

**Rückgabewert**

***positiv*** bei erfolgreichem Weiterleiten der GINA-Anforderung an das GINA-Relay-System
***negativ*** bei fehlgeschlagenem Weiterleiten der GINA-Anforderung an das GINA-Relay-System

**Parameter**

**e-mail-address**
Definiert die E-Mail-Adresse unter welcher das GINA-Relay-System erreichbar ist.

**domainsignature** (optional)
Durch diesen Parameter wird die an das GINA-Relay-System weitergeleitete E-Mail zusätzlich mit einer Domänensignatur - ohne Prüfen des Absenders!!! - versehen.
Geprüft wird auf Empfängerseite (siehe **unpack_mail()** 284) mittels Fingerabdruck des Domänen Zertifikates.
Mögliche Werte:

- true, yes oder 1
- false, no oder 0

default ist 0

**Beispiel**

| Zeile | Code |
|---|---|
| 01 | `if (pack_mail('gina-relay@customer.org', 'yes') {` |
| 02 | `  log(1, 'email successfully sent to remote GINA server');` |
| 03 | `} else {` |
| 04 | `  log(1, 'email could not delivered to remote GINA server');` |
| 05 | `  drop('451', 'Die Nachricht konnte nicht verschluesselt` |
| 06 | `werden');` |
| | `}` |

**Erklärung**
In diesem Beispiel wird die ausgehende E-Mail zur Weiterleitung an ein GINA-Relay-System gepackt, welches unter der (Pseudo) E-Mail Adresse "gina-relay@customer.org" erreichbar ist und mit dem Domainzertifikat signiert (Zeile 1). Erfolg beziehungsweise Misserfolg der Aktion wird protokolliert (Zeile 2 und 4). Bei fehlschlagen der Aktion wird die E-Mail mit dem temporären Fehler "451" und dem Hinweistext "Die Nachricht konnte nicht verschluesselt werden" abgewiesen (Zeile 5).

### 8.7.3.3 unpack_mail()

Der Befehl `unpack_mail()` entpackt auf einem GINA-Relay-System die vom Basis-System übermittelten GINA-Anforderungen.

Mit diesem Befehl werden die vom Basis-System mittels **pack_mail()** 284 übermittelten GINA-

© 2015 SEPPmail AG

Anforderungen angenommen (vergleiche Mail Processing 147 Ruleset Generator **Advanced Options** This is a remote GINA server).
Das weitere Verarbeiten der E-Mail findet im Anschluss statt.

**Aufbau des Befehls**

```
unpack_mail();
```

**Rückgabewert**

***positiv*** immer

**Parameter**

keine

© 2015 SEPPmail AG

#### 8.7.3.4 webmail_keys_avail()

Der Befehl `webmail_keys_avail()` prüft, ob ein GINA-Benutzerkonto vorhanden ist.

**Aufbau des Befehls**

```
webmail_keys_avail();
```

**Rückgabewert**

***positiv*** für die Gruppe mit vorhandenem GINA-Benutzerkonto
***negativ*** für die Gruppe ohne GINA-Benutzerkonto

**Parameter**

keine

**Beispiel**

| Zeile | Code |
|---|---|
| 01 | `if (webmail_keys_avail(){` |
| 02 | `log(1, 'GINA account already exists');` |
| 03 | `} else {` |
| 04 | `log(1, 'no GINA account available, creating new account');` |
| 05 | `webmail_keys_gen('', '8');` |
| 06 | `}` |

**Erklärung**

In diesem Beispiel wird zunächst geprüft, ob ein GINA-Benutzerkonto vorhanden ist (Zeile 1). Das Ergebnis dieser Abfrage wird protokolliert (Zeile 2 und 4). Ist kein GINA-Benutzerkonto vorhanden, so wird ein neues angelegt (Zeile 5).

© 2015 SEPPmail AG

#### 8.7.3.5 webmail_keys_gen()

Der Befehl `webmail_keys_gen()` erstellt ein GINA-Benutzerkonto.

Dieser Befehl generiert ein GINA-Benutzerkonto und schickt das Initial Kennwort an den Absender der ursprünglichen E-Mail oder alternativ an eine optional anzugebende E-Mail Adresse.

**Aufbau des Befehls**

```
webmail_keys_gen(['recipient'], ['password_length'],
['no_pw_email_if_sms_sent']);
```

**Rückgabewert**

***positiv*** immer

**Parameter**

**recipient** (optional)
Definiert die E-Mail Adresse, an welche die E-Mail mit dem Initial Kennwort gesendet werden soll. Wird keine E-Mail Adresse angegeben, so wird die Absender E-Mail Adresse verwendet.

**password_length** (optional)
Definiert die Länge des Initial Kennworts. Dabei steht die "0" (null) für ein leeres Kennwort.
Wird der Parameter nicht angegeben, so wird der Standardwert der Konfigurationsoberfläche (siehe Mail Processing 147 GINA Settings **Password Length**) verwendet.

**no_pw_email_if_sms_sent** (optional)
Mit dieser Option wird die E-Mail mit dem Initial Passwort an den Absender unterbunden, wenn dieses bereits per SMS übermittelt werden konnte (siehe auch Schlüsselwort [SMS:] in Tabelle 1 des Kapitels Steuern der Appliance 86).
Mögliche Werte:

- true, yes oder 1
- false, no oder 0

default ist 0

**Beispiel**

```
webmail_keys_gen('', '8');
```

**Erklärung:**
In diesem Beispiel wird ein GINA-Benutzerkonto erzeugt. Der Absender der ursprünglichen E-Mail erhält eine E-Mail-Benachrichtigung mit dem Initial Kennwort. Dieses Initial Kennwort hat `'8'` (acht) Zeichen.

© 2015 SEPPmail AG

# 8.8 Befehle für LDAP (Zugriff auf externe Quellen)

## 8.8.1 ldap_read

Der Befehl `ldap_read()` liest einen Wert aus einem LDAP-Verzeichnis aus und legt diesen in einer Variablen ab.

Dieser Befehl baut eine Verbindung zu einem LDAP-Server auf, liest den Wert eines Attributs aus und legt diesen in einer Variable ab.
Wird keiner der angegebenen LDAP Server erreicht, so wird die E-Mail mit einem temporären Fehler abgewiesen (420, could not bind to LDAP server).

**Aufbau des Befehls**

```
ldap_read('ldap', 'attr', 'var');
```

**Rückgabewert**

***positiv*** wenn das Attribute `'attr'` gefunden und somit der Variablen `'var'` ein Wert zugewiesen werden kann
***negativ*** wenn der Variablen `'var'` kein Wert zugewiesen werden kann

**Parameter**

**ldap**
Der Parameter ist wie folgt aufgebaut:
'URI;BindDN;Password;SearchBase;Filter'
Die Bedeutung der einzelnen Teil Strings ist der der folgenden Tabelle beschrieben:

| Parameter | Beschreibung |
|---|---|
| URI | Angabe des LDAP Servers, der abgefragt werden soll. Als Eingabe wird der Hostname oder die IP-Adresse aktzeptiert. Es können auch zwei mit Komma getrennte Werte angegeben werden: In diesem Fall wird automatisch auf den zweiten Server zugegriffen, wenn der erste nicht erreicht werden kann. |
| BindDN | Eingabe des vollständigen Distinguished Name (DN) des (read-only) Accounts, welcher zur Suche des unter "SearchBase" in der LDAP Datenbank berechtigt ist. |
| Password | Das Passwort des unter BindDN angegebenen Benutzers |
| SearchBase | Suchpfad: Gibt den Zweig der LDAP Datenbank an, in welchem das Attribute aus dem Parameter `'attr'` zu suchen ist. |
| Filter | Angabe eines Attributes der LDAP Datenbank, unter welchem das gesuchte Attribute aus dem Parameter `'attr'` im Zweig der "SearchBase" zu finden ist. |

**attr**
Attribut nach welchem im LDAP-Verzeichnis gesucht werden soll.

**var**
Name der Variablen, in welcher der Wert des Attributes `'attr'` abgelegt werden soll

**Beispiel**

Der Wert des Attributs "name" soll aus einem LDAP-Verzeichnis ausgelesen werden. Dieser soll in der Variable "name" abgespeichert werden.
Die Anweisung sieht wie folgt aus:

© 2015 SEPPmail AG

```
ldap_read('192.168.10.10;CN=Peter Mueller,OU=SBSUsers,OU=Users,
OU=MyBusiness,DC=Firma,DC=local;mypassword;OU=SBSUsers,OU=Users,
OU=MyBusiness,DC=Firma,DC=local; (mail=$sender)','name','name'););
```

**Erklärung**
Der LDAP Server mit der IP-Adresse 192.168.10.10 (und dem Standardport 389) wird abgefragt.
Der DistinguishedName (DN) des Benutzers unter welchem die Abfrage ausgeführt wird (dieser muss die entsprechenden Berechtigungen besitzen) lautet
CN=Peter Mueller,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local
Das Passwort dieses Benutzers lautet
mypassword
Der LDAP Pfad, in welchem nach dem Attribut "**name**" gesucht werden soll lautet
OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local
Der Benutzer, dessen Gruppenzugehörigkeit festgestellt werden soll, wird anhand der Absender E-Mail Adresse `'ldap/Filter'` definiert.
Existiert das angegebene Attribut `'attr'` oder der gesuchte Eintrag nicht, so wird der Variable `'var'` ein leerer Wert zugewiesen.
Werden mehrere Einträge (Objekte) im Attribut `'attr'` gefunden, so wird nur der erste ausgewertet.
Sollten mehrere Attribute `'attr'` vorhanden sein, so werden alle Attribute ausgewertet (multi value).
Wird keiner der angegebenen LDAP Server erreicht, so wird die E-Mail mit einem temporären Fehler abgewiesen.

© 2015 SEPPmail AG

### 8.8.2 ldap_compare()

Der Befehl `ldap_compare()` vergleicht einen - in einem LDAP-Verzeichnis abgelegten - Wert mit einem angegebenen Attribut.

Dieser Befehl baut eine Verbindung zu einem LDAP-Server auf und prüft den Wert eines Attributs. Wird keiner der angegebenen LDAP Server erreicht, so wird die E-Mail mit einem temporären Fehler abgewiesen (420, could not bind to LDAP server).

**Aufbau des Befehls**

```
ldap_compare('ldap', 'attr', 'value');
```

**Rückgabewert**

***positiv*** wenn der Wert `'value'` für das angegebene Attribute `'attr'` im LDAP Suchstring `'ldap/SearchBase'` gefunden wurde

***negativ*** wenn kein entsprechender Wert gefunden wurde.

**Parameter**

**ldap**

Der Parameter ist wie folgt aufgebaut:

'URI;BindDN;Password;SearchBase;Filter'

Die Bedeutung der einzelnen Teil Strings ist der der folgenden Tabelle beschrieben:

| Parameter | Beschreibung |
|---|---|
| URI | Angabe des LDAP Servers, der abgefragt werden soll. Als Eingabe wird der Hostname oder die IP-Adresse aktzeptiert. Es können auch zwei mit Komma getrennte Werte angegeben werden: In diesem Fall wird automatisch auf den zweiten Server zugegriffen, wenn der erste nicht erreicht werden kann. |
| BindDN | Eingabe des vollständigen Distinguished Name (DN) des (read-only) Accounts, welcher zur Suche des unter "SearchBase" in der LDAP Datenbank berechtigt ist. |
| Password | Das Passwort des unter BindDN angegebenen Benutzers |
| SearchBase | Suchpfad: Gibt den Zweig der LDAP Datenbank an, in welchem das Attribute aus dem Parameter `'attr'` zu suchen ist. |
| Filter | Angabe eines Attributes der LDAP Datenbank, unter welchem das gesuchte Attribute aus dem Parameter `'attr'` im Zweig der "SearchBase" zu finden ist. |

**attr**

Attribut nach welchem im LDAP-Verzeichnis gesucht werden soll.

**value**

Wert, welcher im abgefragten Attribut `'attr'` vorkommen soll.

**Beispiel**

Die Zugehörigkeit des Benutzers "Peter Müller" zur Gruppe "MeineGruppe" soll im LDAP geprüft werden.

Die Anweisung sieht wie folgt aus:

```
ldap_compare('192.168.10.10;CN=Peter Mueller,OU=SBSUsers,OU=Users,
OU=MyBusiness,DC=Firma,DC=local;mypassword;OU=SBSUsers,OU=Users,
OU=MyBusiness,DC=Firma,DC=local;(mail=$sender)','memberOF',
MeineGruppe');
```

© 2015 SEPPmail AG

**Erklärung**
Der LDAP Server mit der IP-Adresse 192.168.10.10 (und dem Standardport 389) wird abgefragt.
Der DistinguishedName (DN) des Benutzers unter welchem die Abfrage ausgeführt wird (dieser muss die entsprechenden Berechtigungen besitzen) lautet
CN=Peter Mueller,OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local
Das Passwort dieses Benutzers lautet
mypassword
Der LDAP Pfad, in welchem nach dem Attribut "**memberOF**" gesucht werden soll lautet
OU=SBSUsers,OU=Users,OU=MyBusiness,DC=Firma,DC=local
Der Benutzer, dessen Gruppenzugehörigkeit festgestellt werden soll, wird anhand der Absender E-Mail Adresse `'ldap_query/Filter'` definiert.
Mindestens ein Wert des Attributes "**memberOF**" muss "**MeineGruppe**" lauten damit der Rückgabewert ***positiv*** ist.
Werden mehrere Einträge `'value'` gefunden, so wird nur der erste ausgewertet.
Sollten mehrere Attribute `'attr'` vorhanden sein, so werden alle Attribute ausgewertet (multi value).
Wird keiner der angegebenen LDAP Server erreicht, so wird die E-Mail mit einem temporären Fehler abgewiesen.

© 2015 SEPPmail AG

### 8.8.3 ldap_getcerts()

Der Befehl `ldap_getcerts()` ruft öffentliche S/MIME Schlüssel (Zertifikate) bei einem LDAP-Verzeichnisdienst ab.

Dieser Befehl ruft für jeden Empfänger einer E-Mail öffentliche S/MIME Schlüssel (Zertifikate) bei einem LDAP-Verzeichnisdienst ab.

**Aufbau des Befehls**

```
ldap_getcerts('ldap');
```

**Rückgabewert**

***positiv*** immer

**Parameter**

**ldap**

Der Parameter ist wie folgt aufgebaut:

'URI;BindDN;Password;SearchBase'

Die Bedeutung der einzelnen Teil Strings ist der der folgenden Tabelle beschrieben:

| Parameter | Beschreibung |
|---|---|
| URI | Angabe des LDAP Servers, der abgefragt werden soll. Als Eingabe wird der Hostname oder die IP-Adresse aktzeptiert. Es können auch zwei mit Komma getrennte Werte angegeben werden: In diesem Fall wird automatisch auf den zweiten Server zugegriffen, wenn der erste nicht erreicht werden kann. |
| BindDN | Eingabe des vollständigen Distinguished Name (DN) des (read-only) Accounts, welcher zur Suche des unter "SearchBase" in der LDAP Datenbank berechtigt ist. |
| Password | Das Passwort des unter BindDN angegebenen Benutzers |
| SearchBase | Suchpfad: Gibt den Zweig der LDAP Datenbank an, in welchem das Attribute aus dem Parameter `'attr'` zu suchen ist. |

**Beispiel**

```
ldap_getcerts('ldap-directory.domain.tld;;;ou=pki-participant,dc=pki,
dc=domain,dc=tld');
```

**Erklärung**

Der LDAP Server, welcher unter dem Fully Qualified Domain Naime (FQDN) "ldap-directory.
domain.tld" (auf dem Standardport 389) erreichbar ist, wird abgefragt.
Ein Benutzer (BindDN) mit Passwort (Password) zur Authorisierung der Abfrage ist nicht notwendig, da es sich im Beispiel um einen öffentlichen LDAP Verzeichnisdienst handelt.
Der LDAP Pfad, in welchem die Zertifikate abliegen lautet

ou=pki-participant,dc=pki,dc=domain,dc=tld

© 2015 SEPPmail AG

### 8.8.4 ldap_getpgpkeys()

Der Befehl `ldap_pgpkeys()` ruft öffentliche openPGP Schlüssel bei einem LDAP-Verzeichnisdienst ab.

Dieser Befehl ruft für jeden Empfänger einer E-Mail öffentliche openPGP Schlüssel bei einem LDAP-Verzeichnisdienst ab.

**Aufbau des Befehls**

```
ldap_getpgpkeys('ldap');
```

**Rückgabewert**

***positiv*** immer

**Parameter**

**ldap**

Der Parameter ist wie folgt aufgebaut:

'URI;BindDN;Password;SearchBase'

Die Bedeutung der einzelnen Teil Strings ist der der folgenden Tabelle beschrieben:

| Parameter | Beschreibung |
|---|---|
| URI | Angabe des LDAP Servers, der abgefragt werden soll. Als Eingabe wird der Hostname oder die IP-Adresse aktzeptiert. Es können auch zwei mit Komma getrennte Werte angegeben werden: In diesem Fall wird automatisch auf den zweiten Server zugegriffen, wenn der erste nicht erreicht werden kann. |
| BindDN | Eingabe des vollständigen Distinguished Name (DN) des (read-only) Accounts, welcher zur Suche des unter "SearchBase" in der LDAP Datenbank berechtigt ist. |
| Password | Das Passwort des unter BindDN angegebenen Benutzers |
| SearchBase | Suchpfad: Gibt den Zweig der LDAP Datenbank an, in welchem das Attribute aus dem Parameter `'attr'` zu suchen ist. |

**Beispiel**

```
ldap_getpgpkeys('ldap-directory.domain.tld;;;ou=pki-participant,dc=pki,
dc=domain,dc=tld');
```

**Erklärung**

Der LDAP Server, welcher unter dem Fully Qualified Domain Naime (FQDN) "ldap-directory.
domain.tld" (auf dem Standardport 389) erreichbar ist, wird abgefragt.
Ein Benutzer (BindDN) mit Passwort (Password) zur Authorisierung der Abfrage ist nicht notwendig, da es sich im Beispiel um einen öffentlichen LDAP Verzeichnisdienst handelt.
Der LDAP Pfad, in welchem die öffentlichen openPGP Schlüssel abliegen lautet

ou=pki-participant,dc=pki,dc=domain,dc=tld

© 2015 SEPPmail AG

## 8.9 Befehle für Content Management

### 8.9.1 iscalendar()

Der Befehl `iscalendar()` prüft eine E-Mail auf das Vorhandensein des Mime-Type **text/calendar**.

Der Befehl prüft, ob es sich bei einer E-Mail um einen Kalendereintrag - zum Beispiel Einladungen, Termine, Besprechungsanfragen - handelt. Diese Abfrage wird typischerweise für das anschliessende Unterbinden kryptographischer Aktionen bei Kalendereinträgen verwendet, da viele E-Mail Clients damit nicht umgehen können.

**Aufbau des Befehls**

```
iscalendar();
```

**Rückgabewert**

***positiv*** wenn die E-Mail den Mime-Type **text/calendar** beinhaltet
***negativ*** wenn die E-Mail den Mime-Type **text/calendar** nicht beinhaltet

**Parameter**

keine

© 2015 SEPPmail AG

### 8.9.2 isspam()

Der Befehl `isspam()` prüft, ob es sich bei einer E-Mail um SPAM handelt.

Dieser Befehl ist nur bei aktiviertem Protection Pack verfügbar. Er prüft den SPAM Level einer E-Mail und führt die entsprechend der eingestellten Schwellwerte definierte Aktion aus (Markieren oder Abweisen).
(siehe auch **Mail Processing** 147 **Ruleset Generator** **Protection Pack (Anti-Spam / Anti-Virus)**).

**Aufbau des Befehls**

```
isspam('marlevel', 'tag', 'rejectlevel');
```

**Rückgabewert**
***positiv*** immer

**Parameter**

**marklevel**
Dieser Parameter definiert den Punktwert, ab welchem eine E-Mail als SPAM E-Mail markiert wird.
Wertebereich: 0.5 - 9.5
Schrittweite: 0.5
Markieren heisst dem Betreff einer E-Mail wird ein entsprechendes Merkmal hinzugefügt. Dieses Merkmal wird mittels dem Parameter `tag` definiert

**tag**
Dieser Parameter definiert einen Wortbestandteil (`tag`) der zur Markierung einer E-Mail als SPAM an den Betreff angehängt wird.

**rejectlevel**
Dieser Parameter definiert den Punktwert, ab welchem eine E-Mail als SPAM E-Mail abgewiesen wird.
Wertebereich: 0.5 - 9.5
Schrittweite: 0.5

**Beispiel**

```
isspam('2.5', '[SPAM]', '4.5');
```

**Erklärung**
In diesem Beispiel wird eine E-Mail auf SPAM überprüft. Wird der SPAM Level von "2.5" erreicht, bleibt jedoch unter "4.5", so wird die E-Mail im Betreff mit dem Hinweis "[SPAM]" gekennzeichnet. Ab Erreichen des Schwellwertes 4.5 wird die E-Mail abgewiesen (rejected).

© 2015 SEPPmail AG

### 8.9.3 vscan()

Der Befehl `vscan()` prüft die gesamte E-Mail auf Viren.

Dieser Befehl ist nur bei aktiviertem Protection Pack verfügbar. Er prüft eine E-Mail auf Viren und sendet eine Benachrichtigung an eine zu definierende E-Mail Adresse.
(siehe auch **Mail Processing** 147 **Ruleset Generator** **Protection Pack (Anti-Spam / Anti-Virus)**).

**Aufbau des Befehls**

```
vscan('notification_e-mail_address');
```

Der Befehl muss mit einem Semikolon abgeschlossen werden.

Dieser Befehl prüft alle Dateianlagen sowie E-Mail Text und Betreff einer E-Mail auf bekannte Viren. Wird ein Virus gefunden, dann wird eine E-Mail-Benachrichtigung an `E-Mail-Addr-für-Benachrichtigung` gesendet. Ein nachfolgender Ruleset-Befehl muss diese E-Mail weiter behandeln.

Der Rückgabewert ist immer dann ***positiv***, wenn das Ergebnis mindestens einer Prüfung der Dateianlagen einer E-Mail positiv (Virenfund) ist, sonst ist er ***negativ***. Der Befehl hat 1 Parameter.

**Parameter**

**notification_e-mail_address**
Definiert die E-Mail-Adresse an welche bei Virenfund eine Benachrichtigung gesendet wird.

**Beispiel**

```
vscan('antivirus-admin@customer.com');
```

**Erklärung**
In diesem Beispiel wird eine E-Mail-Benachrichtigung an 'antivirus-admin@customer.com' gesendet, wenn ein Virus gefunden wurde.

© 2015 SEPPmail AG

## 8.10 Vordefinierte Funktionen

Vordefinierte Funktionen beinhalten gegebenenfalls eine Abfolge von Befehlen, welche für das Realisieren einer bestimmten Funktion von Nöten sind. Dabei werden vor allem variable Werte aus dem Ruleset Generator (siehe **Mail Processing** 147 **Ruleset Generator**) übernommen.
Dadurch kann die Ruleset Programmierung dynamisch auf Änderungen variabler Werte reagieren und wird somit vereinfacht, verkürzt und übersichtlicher.

### 8.10.1 @ADDDISCLAIMER@

Die Funktion `@ADDDISCLAIMER@` hängt die Fussnote an, welche gemäss der **Managed Domain** (siehe "**Mail System** 129 **Managed Domains**" Spalte "**Disclaimer Setting**" der angezeigten Tabelle) zur E-Mail Domäne des Absenders passt.

### 8.10.2 @ARCHIVE@

Die Funktion `@ARCHIVE@` archiviert E-Mails unter Verwendung der unter "**Mail Processing** 147 **Ruleset Generator** **Archiving**" eingetragenen E-Mail Adresse.

### 8.10.3 @CREATEGPGKEYS@

Die Funktion `@CREATEPGPKEYS@` erzeugt für den Absender einer E-Mail ein Schlüsselpaar, so wie es in der Administrationsoberfläche (siehe **Mail Processing** 147 **Ruleset Generator** **Key Generation**) definiert wurde.

**Beispiel**

```
createaccount('@CREATEGPGKEYS@');
```

### 8.10.4 @CREATEUSER@

Die Funktion `@CREATEUSER@` generiert einen neuen Benutzer (siehe **Users** 203), gemäss der Einstellungen wie sie in der Administrationsoberfläche unter **Mail Processing** 147 **Ruleset Generator** **User Creation** definiert wurden, sofern dieser nicht bereits vorhanden ist.

### 8.10.5 @CREATESEPPMAILACCOUNT@

Die Funktion `@CREATESEPPMAILACCOUNT@` generiert einen neuen GINA-Benutzer (siehe **GINA accounts** 210), gemäss der Einstellungen wie sie in der Administrationsoberfläche unter **Mail Processing** 147 **GINA Settings** definiert wurden, sofern dieser nicht bereits vorhanden ist.

© 2015 SEPPmail AG

### 8.10.6 @KEYSERVER@

Die Funktion `@KEYSERVER@` sucht auf den unter "Mail Processing 147 Ruleset Generator **Key Server**" eingetragenen Schlüssel Servern nach öffentlichen Schlüsseln - egal ob openPGP oder S/MIME - für das Verschlüsseln an externe Kommunikationspartner.

**Beispiel**

| Zeile | Code |
|---|---|
| 01 | `@KEYSERVER@` |
| 02 | `if (pgp_keys_avail(){` |
| 03 | `log(1, 'pgp key available');` |
| 04 | `if (encrypt_pgp() {` |
| 05 | `log(1, 'email successfully pgp encrypted');` |
| 06 | `} else {` |
| 07 | `log(1, 'email could not be pgp encrypted');` |
| 08 | `}` |
| 09 | `} else {` |
| 10 | `log(1, 'no pgp key available');` |
| 11 | `}` |

**Erklärung**
In diesem Beispiel wird über @KEYSERVER@ definiert, dass öffentliche Schlüssel - egal ob S/MIME oder openPGP - nicht nur lokal auf der Appliance, sonder auch auf den in der Administrationsoberfläche angegebenen Schlüssel Servern (siehe Mail Processing 147 Ruleset Generator **Key Server**) gesucht werden soll (Zeile 1).
Der Befehl `pgp_keys_avail()` prüft somit sowohl lokal auf der Appliance als auch auf den in der Administrationsoberfläche angegebenen Schlüsselservern, ob ein passender, Benutzer basierter öffentlicher - im Beispiel openPGP - Schlüssel für das Verschlüsseln zur Verfügung steht (Zeile 2). Das Ergebnis dieser Abfrage wird protokolliert (Zeile 3 und 10). Steht ein entsprechender Schlüssel zur Verfügung, wird mit dem Verschlüsseln fortgefahren (Zeile 4), dessen Erfolg beziehungsweise Misserfolg ebenfalls protokolliert wird (Zeile 5 und 7).

### 8.10.7 @REMOVETAGS@

Die Funktion `@REMOVETAGS@` entfernt alle von der Appliance verwendeten tags (Betreffzeilen Schlüsselworte und Kennzeichen) aus einer E-Mail (siehe auch Tabelle 1 des Kapitels Steuern der Appliance 86, in welcher die Standard Schlüsselworte gelistet sind). Dabei werden die im **Ruleset Generator** (siehe Mail Processing 147 Ruleset Generator) vorgenommenen Änderungen der Standard tags berücksichtigt.

### 8.10.8 @REMOVELFMTAGS@

Die Funktion `@REMOVELFMTAGS@` entfernt alle von der Appliance für LFM verwendeten tags (Betreffzeilen Schlüsselworte) aus einer E-Mail, also [LFM] und [LFM:nocrypt] (siehe auch Tabelle 1 des Kapitels Steuern der Appliance 86).

### 8.10.9 @REMOVETAGDECRYPTED@

Die Funktion `@REMOVETAGDECRYPTED@` entfernt das in der Appliance über den **Ruleset Generator** (siehe Mail Processing 147 Ruleset Generator **Encryption/Decryption** Incoming e-mails Add this text to message

© 2015 SEPPmail AG

subject after decryption) festgelegte tag (Betreffzeilen Kennzeichen), welches nach erfolgreichem Entschlüsseln gesetzt wird - im Standard [secure] - aus dem Betreff einer E-Mail.

### 8.10.10 @REMOVETAGSIGNED@

Die Funktion `@REMOVETAGSIGED@` entfernt das in der Appliance über den **Ruleset Generator** (siehe Mail Processing 147 Ruleset Generator **Signing** Incoming e-mails Add this text to message subject if S/MIME signature check succeeds:) festgelegte tag (Betreffzeilen Kennzeichen), welches nach dem erfolgreichen Prüfen einer S/MIME Signatur - im Standard [signed OK] - gesetzt wird, aus dem Betreff einer E-Mail.

### 8.10.11 @REMOVETAGSIGNEDINVALID@

Die Funktion `@REMOVETAGSIGNEDINVALID@` entfernt das in der Appliance über den **Ruleset Generator** (siehe Mail Processing 147 Ruleset Generator **Signing** Incoming e-mails Add this text to message subject if S/MIME signature check fails:) festgelegte tag (Betreffzeilen Kennzeichen), welches nach dem Prüfen einer S/MIME signierten E-Mail mit **ungültiger** Signatur - im Standard ist das [signed INVALID] - gesetzt wird, aus dem Betreff einer E-Mail.

### 8.10.12 @TAGHEADERENCRYPTED@

Die Funktion `@TAGHEADERENCRYPTED@` fügt dem Betreff einer E-Mail das im **Ruleset Generator** (siehe Mail Processing 147 Ruleset Generator **Encryption/Decryption** Incoming e-mails Add this text to message
subject after decryption) eingetragene Schlüsselwort für entschlüsselte E-Mails an.

© 2015 SEPPmail AG

### 8.10.13 @TRIGGERTEXT@

Die Funktion `@TRIGGERTEXT@` gibt das im **Ruleset Generator** angegebene Betreffzeilen Schlüsselwort für das Verschlüsseln (siehe **Mail Processing** 147 **Ruleset Generator** **Encryption/ Decryption** Outgoing e-mails Always encrypt mails with the following text in subject:) aus.

© 2015 SEPPmail AG

## 8.11 Anwendungsbeispiele für das Regelwerk

An dieser Stelle werden Beispiel Codes für explizite Anforderungen bereitgestellt

### 8.11.1 Bounce von E-Mails nicht authentifizierter Benutzer

Wurde zum Beispiel unter **Mail Processing** **Ruleset Generator** **User Creation** die Option "Manual User Creation" gewählt, so werden im Standardverhalten der Appliance E-Mails von Benutzern aus Managed Domains kryptographisch unbehandelt durchgeleitet, wenn diese Absender keinen Benutzer Account (siehe auch **Users** 203) auf der Appliance haben.

Sollen E-Mails dieser Absender entgegen dem Standardverfahren abgewiesen (bounced) werden, so kann dies über einen Custom Command erreicht werden.

**Konfigurationsvorschlag**

- Navigieren zu **Mail Processing** **Ruleset Generator** **Custom Commands** Custom commands for outgoing e-mails BEFORE encryption:
- Anlegen des Templates "bounce_no_user" über **Mail Processing** **Edit Mail Templates**
- Einfügen des folgenden Codes in das Eingabefeld:

```
if (authenticated()) {
} else {
 bounce('bounce_no_user', 'true');
 log(1, 'user account missing');
}
```

**Beschreibung**
Zunächst wird hier geprüft, ob der Absender der E-Mail einen Benutzer Account auf der Appliance besitzt. Ist dies der Fall, so wird das Standard Ruleset weiter ausgeführt. Andernfalls wird die E-Mail abgewiesen (gelöscht) und eine Bounce-Mail an den Absender unter Verwendung der Vorlage "bounce_no_user" und mit dem Header der ursprünlichen ME-Mail an den Absender gesendet.

**Verwendete**
**Befehle**
**authenticated()** 232
**bounce()** 260
**log()** 241

**Funktionen**
keine

**Variationen**
Anstelle des Befehls **bounce()** 260 kann die E-Mail auch über den Befehl **drop()** 263 abgewiesen werden.

© 2015 SEPPmail AG

### 8.11.2 GINA-Verschlüsselung/Tagging zwischen Mandanten erzwingen

Ist die SEPPmail-Appliance als mandantenfähiges System (siehe **Customers**) mit der Anforderung eingerichtet, alle E-Mails mit einem Verschlüsselungskennzeichen zwischen den Mandanten mittels GINA-Technologie zu verschlüsseln, so kann dies zum Beispiel wie folgt realisiert werden.

**Konfigurationsvorschlag**

- Navigieren zu **Mail Processing** Ruleset Generator **Custom Commands** Custom commands for incoming e-mails BEFORE decryption:
- Einfügen des folgenden Codes in das Eingabefeld:

| Zeile | Code |
|---|---|
| | `log(1, 'Start custom commands for incoming e-mails BEFORE');` |
| 01 | `if (from_managed_domain()) {` |
| 02 | `        if (compare('x-smenc', 'equal', 'yes')) {` |
| 03 | `            log(1, 'Encryption requested by plugin, encrypt with` |
| 04 | `GINA');` |
| 05 | `            @REMOVETAGS@` |
| 06 | `            @CREATEUSER@` |
| 07 | `            @CREATESEPPMAILACCOUNT@` |
| 08 | `            if (encrypt_webmail()) {` |
| 09 | `            } else {` |
| 10 | `               log(1, 'webmail encryption failed');` |
| 11 | `               drop ('550', 'Mail not accepted');` |
| 12 | `             }` |
| 13 | `        } else {` |
| 14 | `        }` |
| 15 | `        if (compare('subject', 'substitute', '(?i)` |
| 16 | `@TRIGGERTEXT@')) {` |
| 17 | `            log(1, 'Encryption requested by tag @TRIGGERTEXT@,` |
| 18 | `encrypt with GINA');` |
| 19 | `            @REMOVETAGS@` |
| 20 | `            @CREATEUSER@` |
| 21 | `            @CREATESEPPMAILACCOUNT@` |
| 22 | `            if (encrypt_webmail()) {` |
| 23 | `            } else {` |
| 24 | `               log(1, 'webmail encryption failed');` |
| 25 | `               drop ('550', 'Mail not accepted');` |
| 26 | `             }` |
| 27 | `       } else {` |
| 28 | `       }` |
| 29 | `        if (compare('sensitivity', 'equal', '(?i)` |
| 30 | `companyconfidential')) {` |
| 31 | `            log(1, 'Encryption requested by sensitivity flag,` |
| 32 | `encrypt with GINA');` |
| 33 | `            @REMOVETAGS@` |
| 34 | `            @CREATEUSER@` |
| 35 | `            @CREATESEPPMAILACCOUNT@` |
| 36 | `            if (encrypt_webmail()) {` |
| 37 | `            } else {` |
| 38 | `               log(1, 'webmail encryption failed');` |
| 39 | `               drop ('550', 'Mail not accepted');` |
| 40 | `             }` |
| 41 | `        } else {` |
| 42 | `        }` |
| 43 | `} else {` |
| | `}` |

© 2015 SEPPmail AG

**Beschreibung**
Zunächst wird hier geprüft, ob die E-Mail von einer bekannten Maildomäne (siehe Mail System 129 Managed Domains) stammt (Zeile 2). Im nächsten Schritt wird geprüft, ob vom Absender ein Verschlüsselungsmerkmal gesetzt wurde (Zeile 3, 15, 27). Die folgenden zwölf Anweisungen auf die zuvor genannten Abfragen aus den Zeilen 3, 15 und 27 sind identisch.
So wird der auslösende Trigger protokolliert (Zeile 4, 16, 28) und eventuell weitere vorhandene Betreffzeilen Schlüsselworte und Kennzeichen entfernt (Zeile 5, 17, 29).
Der Absender der E-Mail wird als Benutzer auf der Appliance angelegt, sofern er noch nicht vorhanden ist (Zeile 6, 18, 30). Ebenso wird der oder die Empfänger der E-Mail als GINA-Benutzer angelegt, sofern diese nicht bereits vorhanden sind (Zeile 7, 19, 31).
Danach wird die E-Mail GINA verschlüsselt (Zeile 8, 20, 32). Sollte die GINA-Verschlüsselung fehlschlagen (Zeile 9, 21, 33, so würde dies protokolliert (Zeile 10, 22, 34) und die E-Mail abgewiesen werden (Zeile 11, 23, 35).

**Verwendete**
**Befehle**
log() 241
from_managed_domain() 239
compare() 234
encrypt_webmail() 283
drop() 263

**Funktionen**
@REMOVETAGS@ 298
@CREATEUSER@ 297
@CREATESEPPMAILACCOUNT@ 297
@TRIGGERTEXT@ 300

**Variationen**
Wird der Anweisungsblock

```
@CREATESEPPMAILACCOUNT@
if (encrypt_webmail()) {
} else {
   log(1, 'webmail encryption failed');
   drop ('550', 'Mail not accepted');
}
```

jeweils durch die Funktion @TAGHEADERENCRYPTED@ 299 ersetzt,

```
@TAGHEADERENCRYPTED@
```

so werden statt dem Erzwingen der GINA-Technologie die entsprechenden E-Mails lediglich als sicher gekennzeichnet (Standardkennzeichen ist [secure]).

© 2015 SEPPmail AG

© 2015 SEPPmail AG